MILAN BY TRANSITION NETWORKS®

MIL-SM8002TG

9 Port 10/100/1000BASE-T
Two Combo 1000BASE-X SFP Ports
Advanced Managed Switch

User Guide

Rev.A1

18-SEPT-2006

Regulatory Approval
- FCC Class A
- UL 1950
- CSA C22.2 No. 950
- EN60950
- CE
- EN55022 Class A
- EN55024

Canadian EMI Notice
This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

European Notice
Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community Compliance with these directives imply conformity to the following European Norms:

EN55022 (CISPR 22) - Radio Frequency Interference
EN61000-X - Electromagnetic Immunity
EN60950 (IEC950) - Product Safety

Five-Year Limited Warranty
Transition Networks warrants to the original consumer or purchaser that each of it's products, and all components thereof, will be free from defects in material and/or workmanship for a period of five years from the original factory shipment date. Any warranty hereunder is extended to the original consumer or purchaser and is not assignable.
Transition Networks makes no express or implied warranties including, but not limited to, any implied warranty of merchantability or fitness for a particular purpose, except as expressly set forth in this warranty. In no event shall Transition Networks be liable for incidental or consequential damages, costs, or expenses arising out of or in connection with the performance of the product delivered hereunder. Transition Networks will in no case cover damages arising out of the product being used in a negligent fashion or manner.

Trademarks

The MiLAN logo Transition Networks trademarks are registered trademarks of Transition Networks in the United States and/or other countries.

To Contact Transition Networks

For prompt response when calling for service information, have the following information ready:
- Product serial number and revision
- Date of purchase
- Vendor or place of purchase

You can reach Transition Networks technical support at:

E-mail: support@transition.com
Telephone: +1.800.260.1312 x 200 Fax: +1.952.941.2322
Transition Networks
6475 City West Parkway
Eden Prairie, MN 55344
United States of America

Telephone: +1.800.526.9267
Fax: : +1.952.941.2322

http://www.milan.com
info@ Transition.com

© Copyright 2006 Transition Networks

Content

Introduction **1**
Features 1
Software Features 2
Package Contents 5
Hardware Description **6**
Physical Dimension 6
Front Panel 6
LED Indicators 7
Rear Panel 8
Desktop Installation 8
Power On 8
Network Application **9**
Desktop Application 9
Indoor & Protected Outdoor Application 9
Console Management **9**
Console Management **10**
Connecting to the Console Port 10
Login in the Console Interface 10
CLI Management 13
Commands Level 13
Commands Set List 14
System Commands Set 14
Port Commands Set 16
Trunk Commands Set 20
VLAN Commands Set 21
Spanning Tree Commands Set 23
QOS Commands Set 26
IGMP Commands Set 28
Mac / Filter Table Commands Set 29
SNMP Commands Set 30

Port Mirroring Commands Set....31
Stacking Commands Set....32
802.1x Commands Set....33
TFTP Commands Set....35
Main Menu....36
System Configuration....37
System Information....38
IP Configuration....39
DHCP Configuration....41
DHCP Server Configuration....41
DHCP Client Entries....43
Port and IP Bindings....44
Firmware Update....45
System Event Log....46
System Log Configuration....47
Event Configuration....48
Email Alert Configuration....49
SMTP Configuration....50
Recipient's email Configuration....51
Security Manager....52
Port Configuration....54
Port Counters....54
Port Control Configuration....55
Trunk Configuration....56
Aggregator setting....57
Aggregator Information....58
State Activity....59
Port Mirroring Configuration....60
Rate Limiting....61
Protocol Configuration....63
VLAN Configuration....63

Port Base VLAN Configure 64
Group Add 65
Group Remove 66
Group List 67
802.1Q VLAN Configure 68
GVRP Setting 69
Configure VLAN by Port 70
VLAN List 71
Rapid Spanning Tree 72
RSTP System Configuration 73
RSTP Per Port Configuration 74
SNMP Configuration 76
System Options 77
Community Strings 78
Trap Managers 79
SNMP V 3 Configuration 80
Context Table 81
User Table 82
Group Table 83
Access Table 84
MIBview Table 87
QoS Configuration 90
QoS Policy and Priority Type 91
Default Port Priority 92
COS Configuration 93
TOS Configuration 94
SNTP Configuration 95
IGMP Configuration 98
IGMP Configuration 99
IGMP Status 100
Super ring 100

Security Configuration 102
Security Configuration 103
802.1X/ Radius Configuration 103
System Configuration 104
802.1x Per Port Configuration 105
Misc Configuration 106
Port Security 107
Static MAC Address 108
Filtering MAC Address 109
All MAC Address 110
Load Factory Default Setting 111
Save All Configuration 112
Reboot System 113
Web-Based Management 115
Preparing for Web Management 115
System Login 115
System Information 116
IP Address 117
DHCP Configuration 118
DHCP Server Configuration 119
DHCP Client Entries 120
Port and IP Bindings 120
Update Firmware 121
Restore Configuration 122
Backup Configuration 122
System Log Configuration 123
Event Configuration 124
SMTP Configuration 126
Security Manager 127
Port Statistics 128
Port Control 128

View the Single Port Information 129
Port Trunk 130
Aggregator setting 130
Aggregator Information 131
State Activity 132
Port Mirroring 133
Rate Limiting 134
VLAN configuration 135
Port-based VLAN 136
802.1Q VLAN 138
802.1Q Configuration 140
Group Configuration 140
Rapid Spanning Tree 142
RSTP System Configuration 142
RSTP Per Port Configuration 144
SNMP Configuration 145
System Configuration 145
Trap Managers 147
SNMPV3 Configuration 148
Context Table 148
User Table 148
Group Table 150
Access Table 151
MIBview Table 151
QoS Configuration 152
QoS Policy and Priority Type 152
Port Base Priority 153
COS Configuration 154
TOS Configuration 154
SNTP Configuration 154
IGMP Configuration 157

Super ring 159
Security Configuration 161
802.1X Configuration 161
System Configuration 161
802.1x Per Port Configuration 162
Misc Configuration 163
Port Security 164
Static MAC Address 164
Filtering MAC Address 166
All MAC Address 167
Factory Default 167
Save Configuration 168
System Reboot 168
Troubleshooting 169
Incorrect connections 169
- Faulty or loose cables 169
- Non-standard cables 169
- Improper Network Topologies 170

Diagnosing LED Indicators 170
Technical Specifications 171

Introduction

The product is a multi-port switch that can be used to build high-performance switched indoor or protected outdoor networks. It provides wire-speed, Gigabit Ethernet switching function that allows high-performance, low-cost connection. The Switch features a store-and-forward switching and it can automatically learn and store source address in an 8K-entry MAC address table.

Features

- Nine ports of 10/100/1000BASE-T
- Two SFP 1000BASE-X transceiver slots
- IEEE802.3 10BASE-T, 802.3u 100BASE-TX, 802.3z Gigabit fiber and IEEE 802.3ab 1000Base-T
- IGMP snooping and Query mode support for Multi-Media application
- 18Gbps switch fabric
- 26.7Mpps throughput
- 802.1p CoS, per port 4 queues
- IEEE802.3x Flow control
  - Flow control for full duplex
  - Back pressure for half duplex
- Port Based VLAN /802 .1Q VLAN
- IEEE802.3ad Port trunk with LACP
- Spanning tree protocol
  - Rapid STP
- QoS:
  - Port based / Tag based
  - IPv4 ToS/ Ipv4, IPv6 DiffServe
- Port mirroring and bandwidth control
- IEEE 802.1x user authentication
- GVRP and MVR

- Broadcast storm filter
- DHCP Client, Relay, Server
- Per port band width control
- SNTP and SMTP support
- Management IP address security
- MAC address security
- System log
- SNMP Trap support
- Configuration up-load and down-load
- TFTP firmware update
- Web/SNMP/Telnet/CLI /RMON management

Software Features

Management	SNMP v1, SNMP v2c, SNMP v3, Telnet, Console (Command line interface), Web management and RMON 1(1,2, 3,9)
RFC standard	RFC2233 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 2665 Ethernet like MIB, RFC1215 Trap MIB, RFC 2819 RMON MIB, Private MIB, RFC2030 SNTP, RFC 2821 SMTP, RFC 1757 RMON1 MIB
SNMP Trap	Cold start, warm start, link down, link up, authorization fail, Trap station up to 3.
Software Upgrade	TFTP firmware upgradeable.

Port Trunk	Support IEEE802.3ad with LACP function. Up to 3 trunk groups and maximum group member up to 8 ports.
Spanning Tree	IEEE802.1d Spanning tree IEEE802.1w Rapid spanning tree
VLAN	Port based VLAN Double Tag VLAN for management IEEE802.1Q Tag VLAN. The static VLAN groups up to 256 and dynamic VLAN groups up to 2048, the VLAN ID can be assigned from 1 to 4094. GVRP function supports 256 groups.
Class of Service	Per port supports 4 queues. Wnine round ratio (WRR): High: Mid-High: Mid-Low: Low (8:4:2:1)
Quality of service	Port based, Tag based, IPv4 Type of service, IPv4/IPv6 Different service.
IGMP	IGMP v1 and v2 compliance and also supports 256 IGMP groups and support query mode.
Port Security	It supports ingress and egress MAC address filter and static source MAC address lock.
Port Mirror	Global system supports 3 mirroring types: “RX, TX and Both packet”. The maximum of port mirror entries is up to 8.
Bandwidth Control	Ingress rate limiting packet type: all of frames, broadcast, multicast, unknown unicast and

	broadcast packet. Egress rate shaping supports all of packet. Rate limiting levels: 64kbps to 64Mbits or up to 256Mbits for Gigabit port.
User Authentication	Support IEEE802.1x User-Authentication and can report to RADIUS server. ■ Reject ■ Accept ■ Authorize ■ Disable
System login security	Provide IP management security function and provide 4 accounts.
DHCP	DHCP Client, DHCP relay and DHCP Server. DHCP server provides port based and system based IP pool.
Packet filter	Broadcast storm packet filter by 5%, 10%, 15% and 25%.
System log	Provide 1000 log entries and support remote storage function.
DNS	Support DNS client function.
NTP	Support RFC2030 Simple Network Time Protocol and up to 5 NTP server.
SMTP	Up to 6 mail accounts.

Configuration upload and download	Support binary format configuration file for system quick configuration.

Package Contents

Unpack the contents of the switch and verify them against the checklist below.

- Managed Switch unit
- Power Cord
- Four Rubber Feet
- RS-232 cable
- User Manual

If any item is missing or damaged, please contact your local dealer for service.

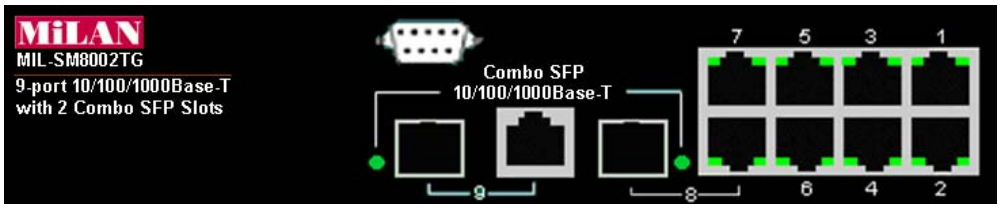
Hardware Description

Physical Dimension

The physical dimensions of the switch is **217mm(W) x 140mm(D) x 43mm(H)**

Front Panel

The Front Panel of the switch consist of 9x auto-sensing 10/100/1000Mbps Ethernet RJ-45 ports (automatic MDI/MDIX), 2 SFP copper combo ports, and the LED indicators are also located on the frond panel of the switch.



Front Panel of the switch

- **RJ-45 Ports (Auto MDI/MDIX):** Nine 10/100/1000 auto- sensing for 10Base-T or 100Base-TX or 1000Base-T connections.

  In general, MDI means connecting to another Hub or Switch while MDIX means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** means that you can connect to another Switch or workstation without changing non-crossover or crossover cabling.

- **2 SFP/Giga copper combo port:** 2 auto detect Giga port—UTP or fiber. Giga fiber is the SFP module that is optional.

LED Indicators

The following table provides descriptions of the LED statuses and meaning. They provide a real-time indication of systematic operation status.

LED	Status	Description
Power	Green	Power On
1000M	Yellow	The port is operating at the speed of 1000Mbps.
	Orange	The port is operating at the speed of 100Mbps.
	Off	The port is operating at the speed of 10Mbps or no device attached
LNK / ACT	Green	The port is successfully connecting with the device.
	Blinks	The port is receiving or transmitting data.
	Off	No device attached.
LNK / ACT (SFP)	Green	The port is successfully connecting with the device.
	Blinks	The port is receiving or transmitting data.
	Off	No device attached.

Rear Panel

The 3-pronged power plug are located at the Rear Panel of the switch as shown in figure. The Switches will work with AC in the range 90-240V AC, 50-60Hz.

Rear Panel of the switch

Desktop Installation

Set the switch on a sufficiently large flat space with a power outlet nearby. The surface where you put your Switch should be clean, smooth, level, and sturdy. Make sure there is enough clearance around the Switch to allow attachment of cables, power cord and air circulation.

Attaching Rubber Feet

1. Make sure mounting surface on the bottom of the Switch is grease and dust free.
2. Remove adhesive backing from your Rubber Feet.
3. Apply the Rubber Feet to each corner on the bottom of the Switch. These footpads can prevent the Switch from shock/vibration.

Power On

Connect the power cord to the power socket on the rear panel of the Switch. The other side of power cord connects to the power outlet. The internal power works with AC in the voltage range 90-240VAC, frequency 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

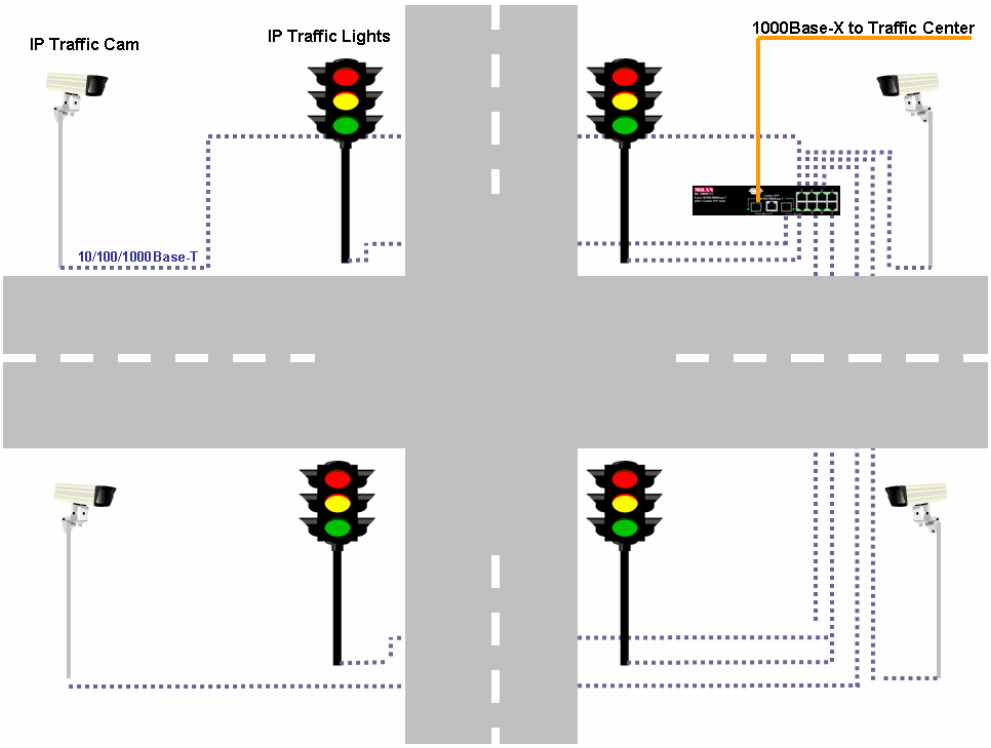
Network Application

Desktop Application

The switch is designed to be a desktop size switch that is an ideal solution for small workgroup. The Switch can be used as a standalone switch to which personal computers, server, printer server are directly connected to form small workgroup.

Indoor & Protected Outdoor Application

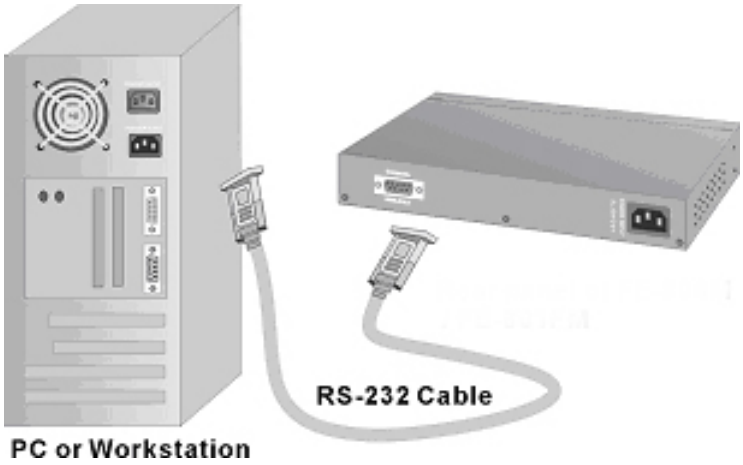
IP based technologies start dominating outdoor applications, that have been historically reserved for serial connectivity. Gigabit switches gradually leave traditional LANs and become a backbone for infrastructure connectivity and management. MIL-SM8002TG switches can interconnect IP-based Traffic control lights, Traffic Cameras and message boards.



Console Management

Connecting to the Console Port

Use the supplied RS-232 cable to connect a terminal or PC to the console port. The terminal or PC to be connected must support the terminal emulation program.

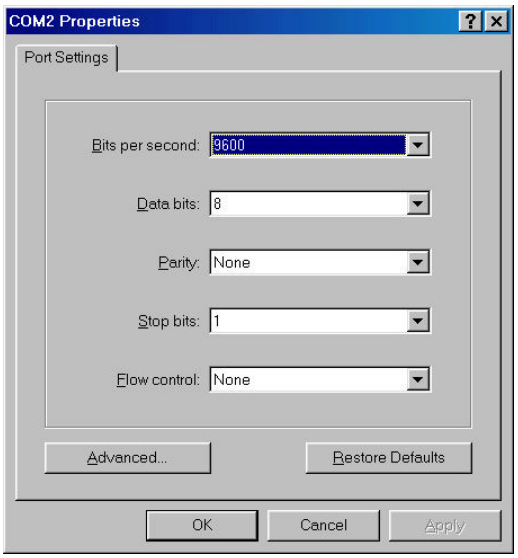


Connecting the switch to a terminal via RS-232 cable

Login in the Console Interface

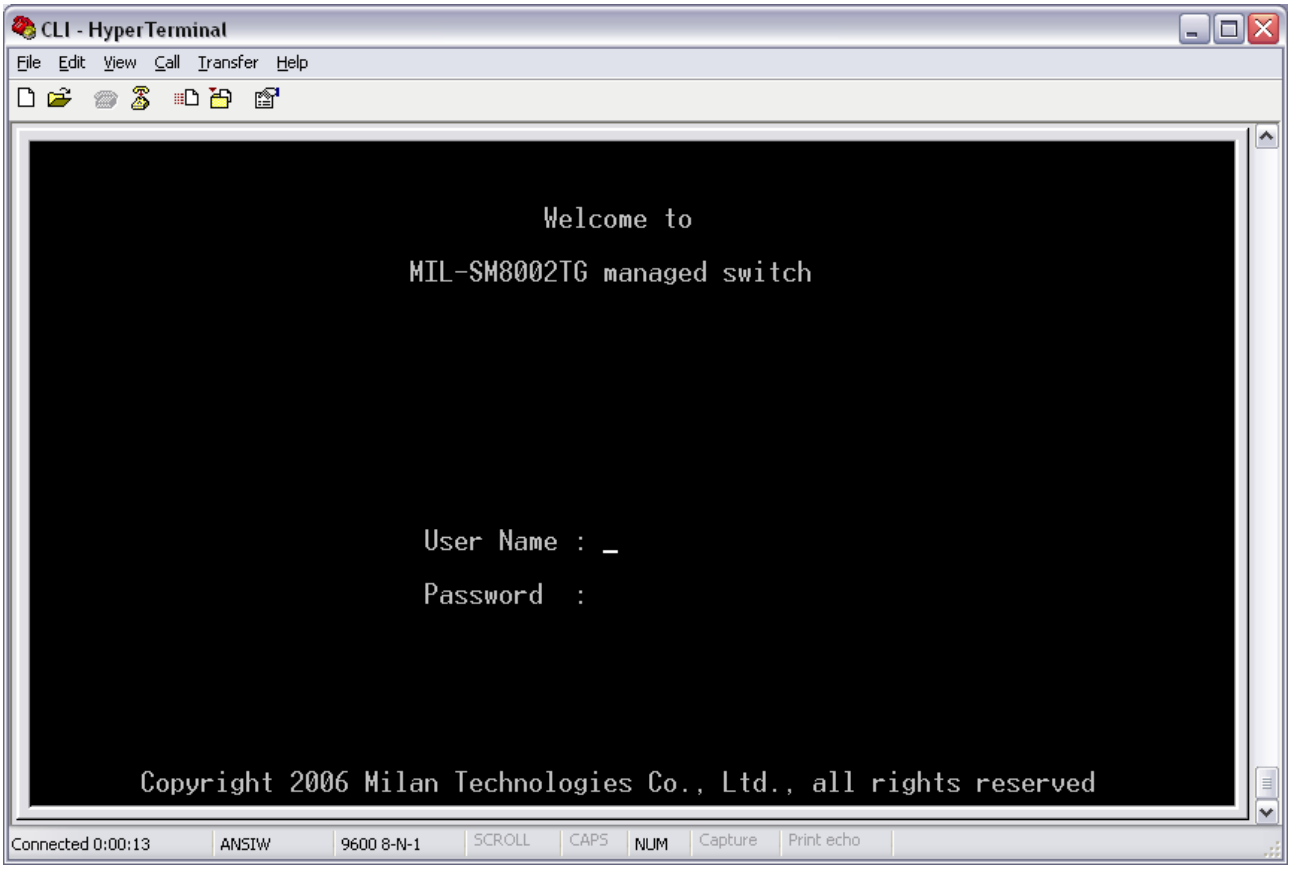
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



The settings of communication parameters

After finished the parameter settings, click "**OK**". When the blank screen shows up, press Enter key to bring out the login prompt. Key in the "**root**"(default value) for the both User name and Password (use **Enter** key to switch), then press Enter key and the Main Menu of console management appears. Please see below figure for login screen.



Console login interface

CLI Management

The system supports two types of console management – CLI command and Menu selection. After you login to the system, you will see a command prompt. To enter CLI management interface, enter "**enable**" command. The following table lists the CLI commands and description.

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode1
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • Save configures
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in global	switch (config-if)#	To exit to global configuration mode, enter exit. To exist to	Use this mode to configure parameters for the switch and Ethernet ports.

	configuration mode		privileged EXEC mode, or end.	

Commands Set List

System Commands Set

Commands	Command Level	Description	Defaults	Example
system name [systemname]	Global configuration mode	Set switch system name string		Switch (config)# system name xxx
system location [system location]	Global configuration mode	Set switch system location string		Switch (config)# system location LA
system description [systemdescription]	Global configuration mode	Set switch system description string		Switch (config)# system description xxx
system contact [systemcontact]	Global configuration mode	Set switch system contact window string		Switch (config)# system contact John
ip address [ip-address] [subnet-mask] [gateway]	Global configuration mode	Use the ip address interface configuration command to set an IP address for a switch. Use the no form of this command to remove an IP address or to disable IP processing.		Switch (config)# ip address 192.168.1.77 255.255.255.0 192.168.1.254

reload	Global configuration mode	Halt and perform a cold restart		Switch (config)# reload
default	Global configuration mode	Restore to default		Switch (config)# Default
username [user-name]	Global configuration mode	Changes a login username. (maximum 10 words)		Switch (config)# username xxxxxx
password [password]	Global configuration mode	Specifies a password (maximum 10 words)		Switch (config)# Password xxxxxx
show system info	User EXEC	Show system information		Switch> show system info Name: switch1 location: lab Description: layer2 switch Contact: somewhere Serial NO: 1.00
show ip	Privileged EXEC	Show ip information		Switch# show ip Address ip: 192.168.1.77 Address subnet: 255.255.255.0 Address gateway: 192.168.1.254

show accounting	Privileged EXEC	Show username & password		Switch# show accounting Username: root Password: root
show version	User EXEC	Use the show version user EXEC command to display version information for the hardware and firmware.		Switch> show version Firmware version: 1.0 Hardware version: 3.0 Kernel version: 1.10
show terminal	Privileged EXEC	Use the show terminal command to display console information for the switch		Switch (config)# show terminal Baud rate (bits/sec): 9600 Data Bits: 8 Parity Check: none Stop Bits: 1 Flow Control: none

Port Commands Set

Commands	Command Level	Description	Defaults	Example
interface [FastEthernet /module Ethernet] [slot id] [id]	Interface configuration mode	Use the fast Ethernet interface configuration command		Switch (config)# interface fastEthernet 0/1
		Use the module Ethernet interface configuration command		Switch (config)# interface moduleEthernet 1/1

duplex [full | half| auto]	Interface configuration mode	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	Auto	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# duplex full
		Use the duplex configuration command to specify the duplex mode of operation for module Ethernet.	Auto	Switch (config)# interface moduleEthernet 1/1 Switch (config-if)# duplex full
speed [10 | 100 | 1000 | auto]	Interface configuration mode	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet.	Auto	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# speed 10
speed [10| 100 | 1000 | auto]	Interface configuration mode	Use the speed configuration command to specify the speed mode of operation for module Ethernet. (The 100Base-FX module only supported for speed 100) (The 1000Base-FX module only supported for speed 1000 & auto)		Switch (config)# interface fastEthernet 1/2 Switch (config-if)# speed 1000

flowcontrol on or no flowcontrol	Interface configuration mode	Use the flow control configuration command on Ethernet ports to control traffic rates during congestion. Use the no form of this command to disable security on the port.	On	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# flowcontrol on
security on or no security	Interface configuration mode	Use the security configuration command on Ethernet ports. Use the no form of this command to disable security on the port.	Disable	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# security on
priority on [hi | low] or no priority	Interface configuration mode	Use the priority configuration command on Ethernet ports. Use the no form of this command to disable security on the port.	Disable	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# priority on hi
Bandwidth [in | out] [value]	Interface configuration mode	Set bandwidth in or out rate. The value rage is (0~999), and zero of the value is disable (The module can't be setting)	Disable	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# bandwidth in 50

State [Enable | Disable]	Interface configuration mode	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	Enable	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# state disable
show interface configuration	Interface configuration mode	show interface configuration status		Switch (config)# interface fastEthernet 0/1 Switch (config-if)# show interface configuration
show interface status	Interface configuration mode	show interface actual status		Switch (config)# interface fastEthernet 0/1 Switch (config-if)# show interface status
show interface accounting	Interface configuration mode	show interface statistic counter		Switch (config)# interface fastEthernet 0/1 Switch (config-if)# show interface accounting

show bandwidth	Interface configuration mode	Display the bandwidth of the values		Switch (config)# interface fastEthernet 0/1 Switch (config-if)# Show bandwidth

Trunk Commands Set

Commands	Command Level	Description	Defaults	Example
port group [group-number] [port-list] lacp [on | off] workp [work ports] no port group [group-number] lacp [on | off] workp [work ports]	Global configuration mode	Add trunking group. Use the no form of this command to delete trunking group.	Disable	LACP: Switch (config)# port group 1 1-4 lacp on workp 2 Trunk without LACP: Switch (config)# port group 1 1-4 lacp off workp 4
show group [group-ID]	Privileged EXEC mode	Display trunk group information. If there is no group-number in put, display all trunk groups.		Switch # show group 1 Group Trunk.1: Ports: 02 03 04 Priority: 0001 Lacp: Enable Work ports: 0
port group [group-number] activityport [port-list]	Global configuration mode	Set trunking group port active		Switch (config)# port group 3 activityport 2-4 Trunk.1 Lacp: Enable

				Check OK! NEW: 2 4 Update finished!!

VLAN Commands Set

Commands	Command Level	Description	Defaults	Example
Vlan datatbase	Privileged EXEC mode	To enter the VLAN configuration interface		Switch# vlan database Switch(vlan)#
vlanmode [disable| portbase| 802.1q | gvrp]	VLAN database mode	To set switch VLAN mode .Use the no form of this command to restore to default.	Disable	Switch (vlan)# vlanmode 802.1q
Port Base VLAN				
vlan [Group Name] grpid [Group ID] port [Port Number]	VLAN database mode	Add new Port Base VLAN		Switch (vlan)# vlan v2 grpid 2 port 1-4
no vlan Group Name] [Group ID]	VLAN database mode	Delete port base VLAN group		Switch (vlan)# no vlan v2 2
show vlan [GroupName] [GroupID] or show vlan	VLAN database mode	Show VLAN of Group Name or Group ID information		Switch (vlan)# Show vlan v2 2
vlan [Group name] add [port Number] [tagged | untagged]	VLAN database mode	Set the port of some port group tagged or untagged		Switch (vlan)# vlan v2 add 5 tagged
vlan [Group name] delete [port Number]	VLAN database mode	Remove the port from it's port group.		Switch (vlan)# vlan v2 delete 5
802.1Q | 802.1Q with GVRP VLAN mode				
vlan [Group name] vlanid [Vlan ID] port [port Number] tag [port Number]	VLAN database mode	Add new 802.1Q VLAN [VLAN name]: VLAN name [VLAN ID]: 1 ~ 4094 [port ID]: port members 1~9		Switch(vlan)# vlan v2 vlanid 2 port 1-4 tag 2-4
no vlan	VLAN database	Delete 802.1Q VLAN group		Switch (vlan)# no vlan v2

[Group name] or [VLAN ID]	mode			Switch (vlan)# no vlan v2 2
vlan protocol [Group name] [protocol value] vlanid [VLAN ID] port [portNumber] tag [port Number]	VLAN database mode	Add protocol vlan [Group name]: vlan group name [protocol value] IP-ip , ARP-arp, Appletalk_AARP-app_arp , Novell_IPX-ipx , Banyan_vines-banyan_c4, Banyan_vines-banyan_c5, Banyan_vines-banyan_ad, Decent_mop_01-decent_01, Decent_mop_02-decent_02, Decent_dpr-decent_dpr, Decent_LAT-decent_lat, Decent_LAVC-decent_larc, IBM SNA-ibm, X.75 internet-x75, X.25 Layer3-x25 [VLAN ID]: 1 ~ 4094 [port Number]: port Number 1~24	6510,6526	Switch (vlan)# vlan protocol v3 ip vlanid 2 port 5-8 tag 6,8
vlanidrange [VLANidrange]	VLAN database mode	Set VLAN ID range [1~255] range 0 [256~511] range 1 [512~767] range 2 [768~1023] range 3 [1024~1279] range 4 [1280~1535] range 5 [1536~1791] range 6 [1792~2047] range 7 [2048~2303] range 8 [2304~2559] range 9 [2560~2815] range 10 [2816~3071] range 11 [3072~3327] range 12 [3328~3583] range 13		Switch (vlan)# vlanidrange 2 OLD: 0 NEW: 2

		[3584~3839] range 14 [3840~4094] range 15		
VLAN protocol [Groupname] add [portNumber] [tagged | untagged]	VLAN database mode	Set the port of some port group tagged or untagged		Switch (vlan)# vlan protocol v2 add 5 tagged
VLAN protocol [Groupname] delete [portNumber]	VLAN database mode	Remove the port from its port group.		Switch (vlan)# vlan protocol v2 delete 5
show vlan [Groupname] [GroupID] or show vlan	VLAN database mode	Show VLAN of Group Name or VLAN ID information vlanid: 1 ~ 4094		Switch (vlan)# show vlan v2 2
show vlan protocol	VLAN database mode	show protocol vlan Protocol ip ipx netbios		Switch (vlan)# show vlan protocol
port [port ID] pvid [port VID] ingressfilter1 [on | off] ingressfilter2 [on | off]	VLAN database mode	Set Port PVID and Ingress Filter Rules1 & Ingress Filter Rules2		Switch (vlan)# port 2 pvid 2 ingressfilter1 off ingressfilter2 on
show port [port ID]	VLAN database mode	show Port PVID and Ingress Filter Rules1 & Ingress Filter Rules2		Switch (vlan)# show port 2 Port ID: 2 Port Vid: 2 Ingress 1 Filter: Disable Ingress 2 Filter: Enable

Spanning Tree Commands Set

Commands	Command Level	Description	Defaults	Example
show spanning-tree	User EXEC mode	Display a summary of the spanning-tree states.		Switch> show spanning-tree System: Priority: 32768 Max Age: 20 Hello Time: 2 Forward Delay: 15

				Priority: 32768 Mac Address: 004063800030 Root_Path_Cost: 0 Root Port: we are root Max Age: 20 Hello Time: 2 Forward Delay: 15
spanning-tree [on / off] or no spanning-tree	Global configuration mode	Use the spanning-tree global configuration command to enable Spanning Tree Protocol (STP). Use the no form of the command to restore to default	Disable	Switch (config)# spanning-tree on
spanning-tree priority [number]	Global configuration mode	Use the spanning-tree max-age global configuration command to change the priority. Use the no form of this command to return to the default interval.	32768	Switch (config)# spanning-tree priority 32767
spanning-tree max-age [seconds]	Global configuration mode	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol	20 sec	Switch (config)# spanning-tree max-age 15

		data unit (BPDU) message from the root switch within this interval, it recomputes the Spanning Tree Protocol (STP) topology. Use the no form of this command to return to the default interval.		
spanning-tree hello-time [seconds]	Global configuration mode	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs). Use the no form of this command to return to the default interval.	2 sec.	Switch (config)# spanning-tree hello-time 3
stp-path-cost [PortCost]	Interface configuration mode	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state. Use the no form of this command to return to the default value.	10 Mbps – 100 100 Mbps – 10	Switch (config)# interface fastEthernet 0/2 Switch (config-if)# stp-path-cost 20
spanning-tree forward-time [seconds]	Global configuration mode	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and	15 sec.	Switch (config)# spanning-tree forward-time 20

		learning states last before the port begins forwarding. Use the no form of this command to return to the default value.		
stp-path-priority [Port Priority]	Interface configuration mode	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch. Use the no form of this command to return to the default value.	128	Switch (config)# interface fastEthernet 0/2 Switch (config-if)# stp-path-priority 127

QOS Commands Set

Commands	Command Level	Description	Defaults	Example
qos storm-control [5|10|15|20|25| off (%)] or no storm-control	Global configuration mode	Enable/Disable broadcast storm control. Use the no form of this command to restore to default.	OFF	Switch (config)# qos storm-control 5
qos low-priority-delay-bound [on|off] [sec.] or no qos low-priority-delay-bound	Global configuration mode	Enable/Disable low priority delay board. Use the no form of this command to restore to default.	OFF	Switch (config)# qos low-priority-delay-bound on 1
qos level [priority] enable	Global configuration mode	[Priority] 0~7	0~3 LOW 4~7 HI	Switch (config)# qos level 2,3 enable

no qos level [priority]	Global configuration mode	[Priority] 0~7	0~3 LOW 4~7 HI	Switch (config)# no qos level 0-7
qos queuepolicy [Policy] hi [Priority] low [Priority]	Global configuration mode	[Policy]:fcfs: first in and first out wrr: wnine round robin sp: all high before low. [Priority] Hi:1~7 Low:1	WRR Hi 2 Low 1	WRR: Switch (config)# qos queuepolicy wrr hi 7 low 1 First Come First Served: Switch (config)# qos queuepolicy fcfs All High before Low: Switch (config)# qos queuepolicy sp
qos bridge-delay-bound [number] . no qos bridge-delay-bound	Global configuration mode	Set qos bridge delay bound Use the no form of this command to restore to default.	OFF	Switch (config)# qos bridge-delay-bound 1
show qos storm-control	Global configuration mode	Show broadcast storm control.		Switch (config)# show qos storm-control QOS storm control mode: ENABLE

show qos low-priority-delay-bound	Privileged EXEC mode	Show low priority delay board.		Switch (config)# show qos low-priority-delay-bound Qos low priority delay bound: 1
show qos policy	Privileged EXEC mode	Show qos policy		Switch (config)# show qos policy Qos Mode: WRR
show qos bridge-delay-bound	Privileged EXEC mode	Show bridge delay bound		Switch (config)# show qos bridge-delay-bound bridge-delay-bound 5

IGMP Commands Set

Commands	Command Level	Description	Defaults	Example
igmp [on | off]	Global configuration mode	Enable /Disable IGMP snooping function	Off	Switch (config)# igmp on
Igmp-query [auto |enable | disable]	Global configuration mode	Modify IGMP query mode	Disable	Switch (config)# Igmp-query enable
show ip igmp profile	Privileged EXEC mode	Displays the details of an IGMP profile entry.		Switch# show ip igmp profile IP VID Port 224.1.1.1 10 1,2,6

Mac / Filter Table Commands Set

Commands	Command Level	Description	Defaults	Example
mac-address-table aging-time [on | off] mac-address-table aging-time [sec.] or no mac-address-table aging-time	Global configuration mode	Use the mac-address-table aging-time global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the no form of this command to use the default aging-time interval. The aging time applies to all VLANs.	300 secs	(Enable) Switch (config)# mac-address-table aging-time on Switch (config)# mac-address-table aging-time 333 (Disable) Switch (config)# mac-address-table aging-time off Or Switch(config)# no mac-address-table aging-time
mac-address-table table [static | filter] hwaddr [MAC address] vlanid [VLAN-ID]	Interface configuration mode	Use the mac-address-table static to add static | filter addresses to the MAC address table. Use the no form of this command to remove static entries from the MAC address table.	N/A	Switch (config)# interface fastEthernet 0/2 Switch (config-if)# mac-address-table static hwaddr 004063112233 vlanid 10
no mac-address-table [static | filter] hwaddr [MAC address] vlanid [VLAN-ID]	Interface configuration mode	Use the no mac-address-table privileged EXEC command to delete entries from the MAC address table.		Switch (config)# interface fastEthernet 0/2 Switch (config-if)# no mac-address-table static hwaddr 004063112233 vlanid 10

show mac-address-table [static | filter]	Privileged EXEC mode	Use the show mac-address-table user EXEC command to display the MAC address table.		Switch (config)# show mac-address-table static
show mac-address-table aging-time	Privileged EXEC mode	Use the show mac-address-table user EXEC command to display the MAC address table.		Switch (config)# show mac-address-table aging-time 300 MAC Address aging-time: 300

SNMP Commands Set

Commands	Command Level	Description	Defaults	Example
snmp system-name [SystemName]	Global configuration mode	Set Snmp agent system name	N/A	Switch (config)# snmp system-name l2switch
snmp system-location [SystemLocation]	Global configuration mode	Set Snmp agent system location	N/A	Switch (config)# snmp system-location lab
snmp system-contact [SystemContact]	Global configuration mode	Set Snmp agent system contact	N/A	Switch (config)# snmp system-contact where
snmp community-strings [Community] right [RO | RW] Or no snmp community-strings [Community]	Global configuration mode	Add snmp community string. Use the no form of this command to remove the specified community.	PUBLIC RO	Switch (config)# snmp community-strings public right RW

Port Mirroring Commands Set

Commands	Command Level	Description	Defaults	Example
port monitor [RX|TX|Both |Disable] PortList Or no port monitor	Interface configuration mode	Use the port monitor interface configuration command to enable Switch Port Analyzer (SPAN) port monitoring on a port. Use the no form of this command to return the port to its default value.	N/A	Switch (config)# Interface fastEthernet 0/8 Switch (config-if)# port monitor both 3
show port monitor	Interface configuration mode	Use the show port monitor privileged EXEC command to display the ports for which Switched Port Analyzer (SPAN) port monitoring is enabled.		Switch (config-if)# show port monitor State: ENABLE AnalysisPortId: 8 Port 1 Rx: Monitor Port 1 Rx: Monitor Port 2 Rx: Port 2 Rx: Port 3 Rx: Monitor Port 3 Rx: Monitor Port 4 Rx: Port 4 Rx: Port 5 Rx: Port 5 Rx: Port 6 Rx: Port 6 Rx: Port 7 Rx: Port 7 Rx: Port 8 Rx: Analysis Port 8 Tx: Analysis Port 9 Rx: Port 9 Rx:

Stacking Commands Set

Commands	Command Level	Description	Defaults	Example
show stackinglist	User EXEC	Show IP stacking List		Switch>show stackinglist MAC = 00:22:33:44:55:66 [Master] No Slave!
show stackinginfo [MAC address]	User EXEC	Show the stack information		Switch>show stackinginfo 00.22.33.44.55.66 GroupID: 3000 Stacking Mode: Disable System Information: test
stacking [MAC address]	User EXEC	Change to stacking mode		Switch>stacking 00.22.33.44.55.66 Switch(stacking-00.22.33.44.55.66)#
set idmode [ID] [mode]	Stacking Mode	Set the stack ID and mode ID range: 0~65535 Mode: 0 = Disable, 1 = Master, 2 = Slave		Switch(stacking-00.22.33.44.55.66)# set idmode 3000 0 Setting GroupID: 3000, stacking Mode = Disable
set information [name]	Stacking Mode	Set the information of the Stack		Switch(stacking-00.22.33.44.55.66)# set information test Setting System Information: test

802.1x Commands Set

Commands	Command Level	Description	Defaults	Example
show 8021x	User EXEC mode	Display a summary of the 802.1x properties and also the port sates.		Switch> show 8021x
8021x [on | off]	Global configuration mode	Use the 802.1x global configuration command to enable 802.1x protocols. Use the no form of the command to restore to default	Disable	Switch (config)# 8021x on
8021x system radiusip [RadiusServerIP] Or no 8021x system radiusip	Global configuration mode	Use the 802.1x system radius IP global configuration command to change the radius server IP. Use the no form of this command to return to the default interval.		Switch (config)# 8021x system radiusip 192.168.1.254
8021x system sharekey [Sharekey] or no 8021x system sharekey	Global configuration mode	Use the 802.1x system sharekey global configuration command to change the shared key value. Use the no form of this command to return to the default interval.		Switch (config)# 8021x system sharekey 123456
8021x misc quietperiod	Global	Use the 802.1x misc quiet period		Switch (config)# 8021x

[quietperiod value] Or no 8021x misc quietperiod	configuration mode	global configuration command to specify the quiet period value of the switch. Use the no form of this command to return to the default interval.		misc quietperiod 10
8021x misc txperiod [TXPeriod value] Or no 8021x txperiod	Global configuration mode	Use the 802.1x misc TX period global configuration command to set the TX period. Use the no form of this command to return to the default value.		Switch (config)# 8021x misc txperiod 5
8021x misc supptimeout [SEC] Or no 8021x supptimeout	Global configuration mode	Set the period of time the switch wait for a supplicant response to an EAP request.		Switch(config)# 8021x misc supptimeout 30
8021x misc servertimeout [SEC] Or no 8021x servertimeout	Global configuration mode	Set the period of time the switch wait for a server response to an authentication request.		Switch(config)# 8021x misc servertimeout 50
8021x misc maxrequest [Number] Or no 8021x maxrequest	Global configuration mode	Set the number of authentication that must time-out before authentication fails and the authentication session ends.		Switch(config)# 8021x misc maxrequest 2
8021x misc reauthperiod [SEC] Or no 8021x reauthperiod	Global configuration mode	Set the period of time after which clients connected must be re-authenticated..		Switch(config)# 8021x misc reauthperiod 20
8021x prostate [reject | accept | authorize | disable]	Interface configuration mode	Use the 802.1x port state interface configuration command to set the state of the selected port. ■ **Reject:** the specified port is required to be held in the unauthorized state. ■ **Accept:** the specified port is required to be held in the Authorized state. ■ **Authorized:** the specified port is		Switch (config)# interface fastethernet 0/3 Switch (config-if)# 8021x portstate accept

		set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server. ■ **Disable:** The specified port is required to be held in the Authorized state.		

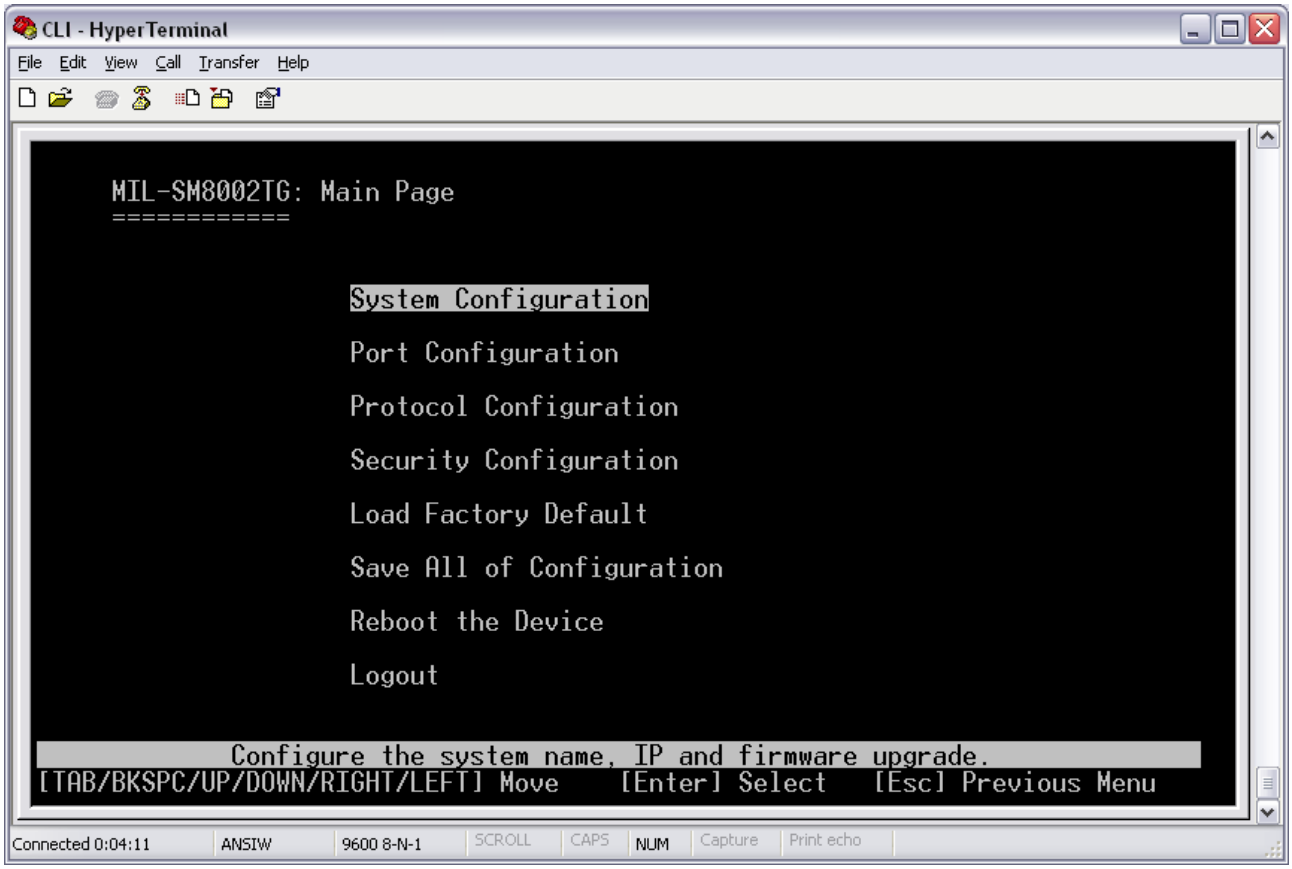
TFTP Commands Set

Commands	Command Level	Description	Defaults	Example
copy flash:config.text tftp [TFTP IP address] [file name]	Global configuration mode	Backup configure file command		Switch (config)# copy flash:config.text tftp >192.168.1.1 >backup.dat
tftp:config.text flash [TFTP IP address] [file name]	Global configuration mode	Restore configure file command		Switch(config)# Tftp:config.text flash >192.168.1.1 >restore.dat
tftp:firmware flash [TFTP IP address] [file name]	Global configuration mode	Update firmware command		Switch (config)# Tftp:firmware flash >192.168.1.1 >image.bin

Main Menu

There are five selections as follow.

- **System Configuration:** Configure system information, IP, DHCP, login security, event logs and firmware update.
- **Port Configuration:** Display port statistics. Configure the port control, trunk, rate limiting and mirroring.
- **Protocol Configuration:** Configure VLAN, RST, SNMP, QoS, SNTP, IGMP, and Super Ring function.
- **Security Configuration:** Configure 802.1X, IP, and Port security function.
- **Load Factory Default:** Reset switch to default configuration.
- **Save All Configuration:** Save the configuration that user had made in the switch system.
- **Reboot the Device:** Reboot the switch system without reset to the default value.
- **Logout:** Exit the menu line program.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Main Page
System Configuration
Port Configuration
Protocol Configuration
Security Configuration
Load Factory Default
Save All of Configuration
Reboot the Device
Logout
Configure the system name, IP and firmware upgrade.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:04:11 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Main menu line interface

- **Control Key description:**

The control keys provided in all menus:

Tab: Move the vernier to next item.

Backspace: Move the vernier to previous item.

Enter: Select item.

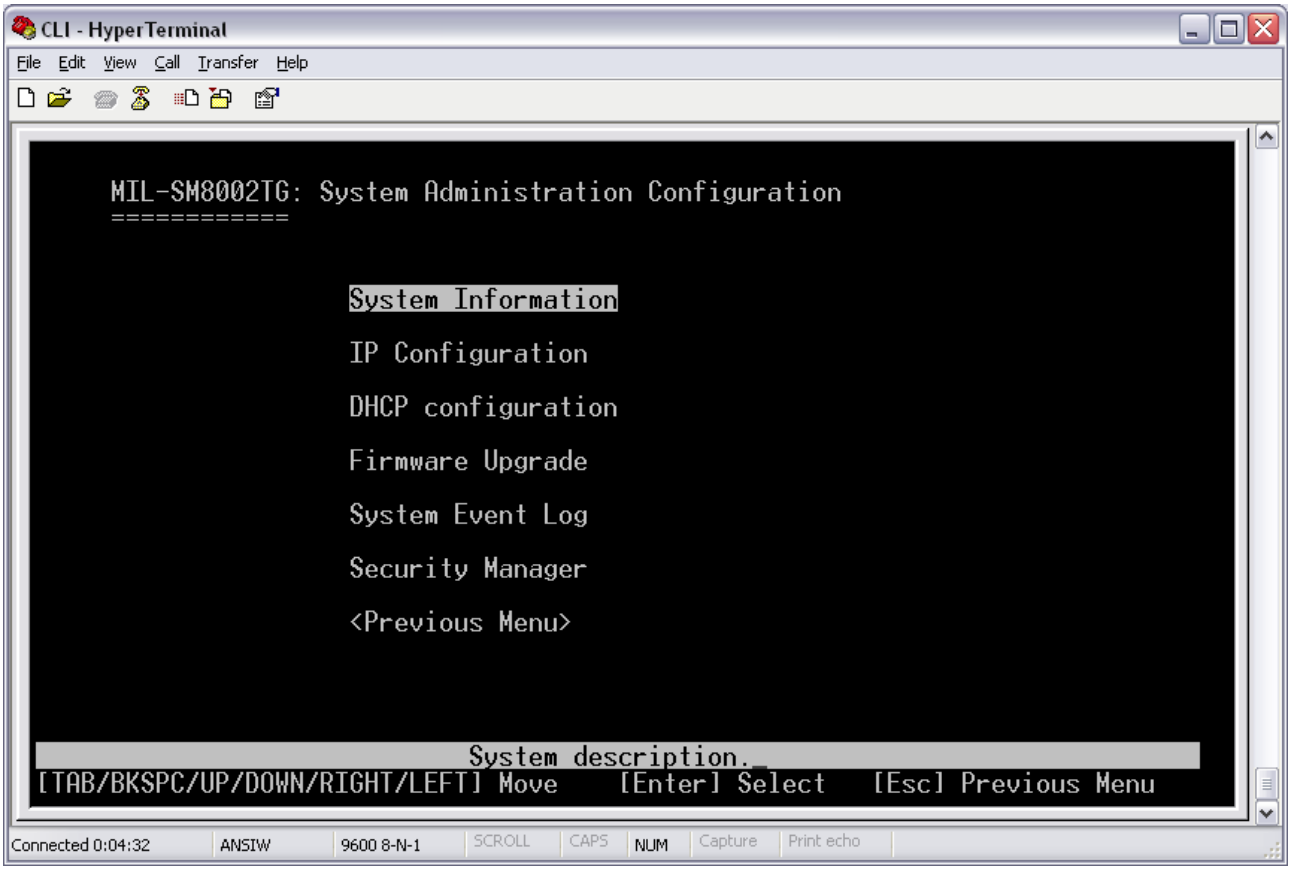
Space: Toggle selected item to next configure or change the value.

Esc: to exit the current action mode.

System Configuration

In System Configuration, you can configure system event log, SMTP, system description, IP, DHCP, login security and firmware update. You can press the “**Tab**” or “**Backspace**” to

choose the item, and press “**Enter**” key to select the item.



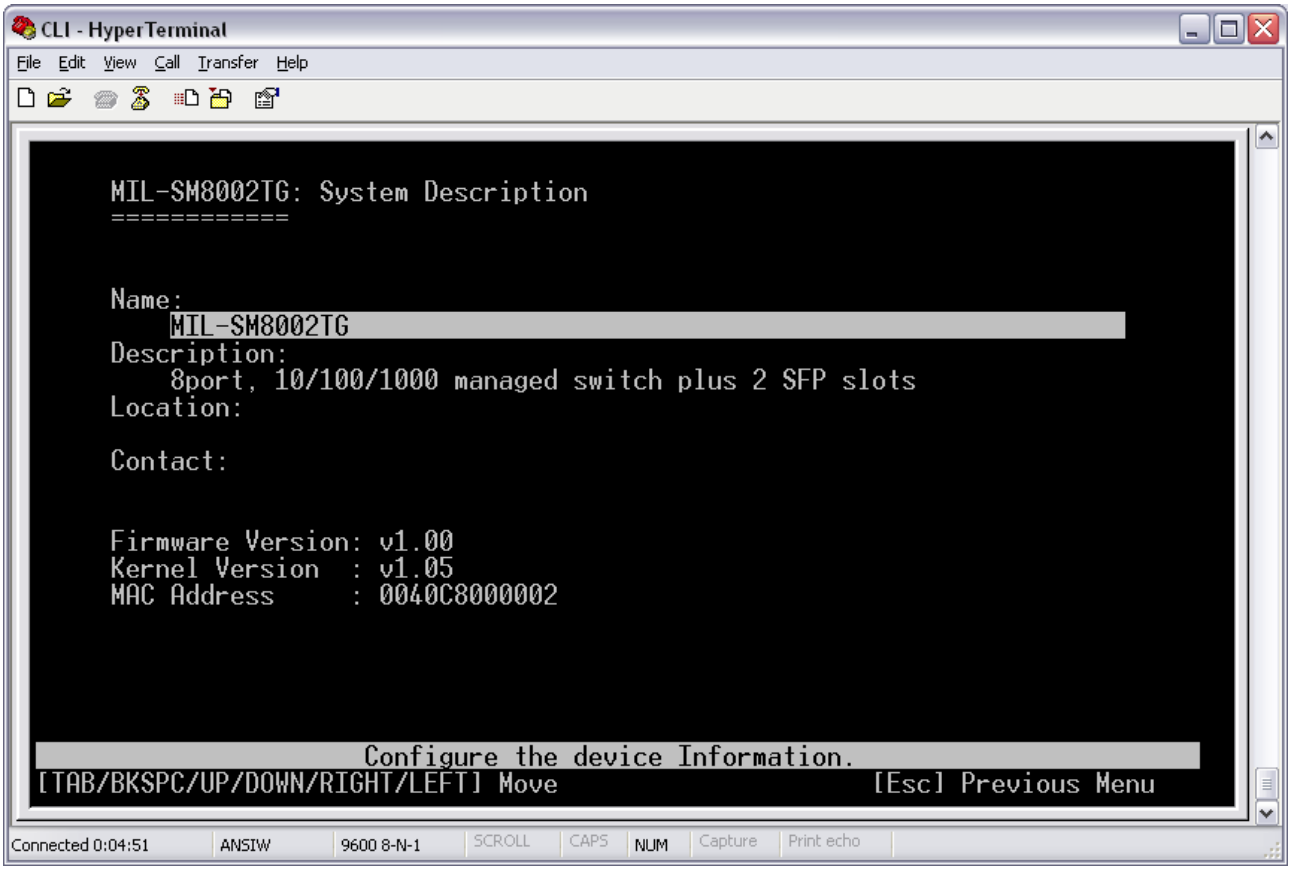
Status and Counters main configuration interface

System Information

You can configure the name, description, location, contact of the system. Also, you can view the version of firmware, hardware, kernel and MAC address.

1. **Name:** the name of device.
2. **Description:** the name of device type.
3. **Location:** where the device is located.
4. **Contact:** the contact person or information.
5. **Firmware Version:** the switch’s firmware version.
6. **Hardware Version:** the switch’s Hardware version.
7. **Kernel Version:** the system kernel software version.

8. **MAC Address:** The unique hardware address assigned by manufacturer.



System Description interface

IP Configuration

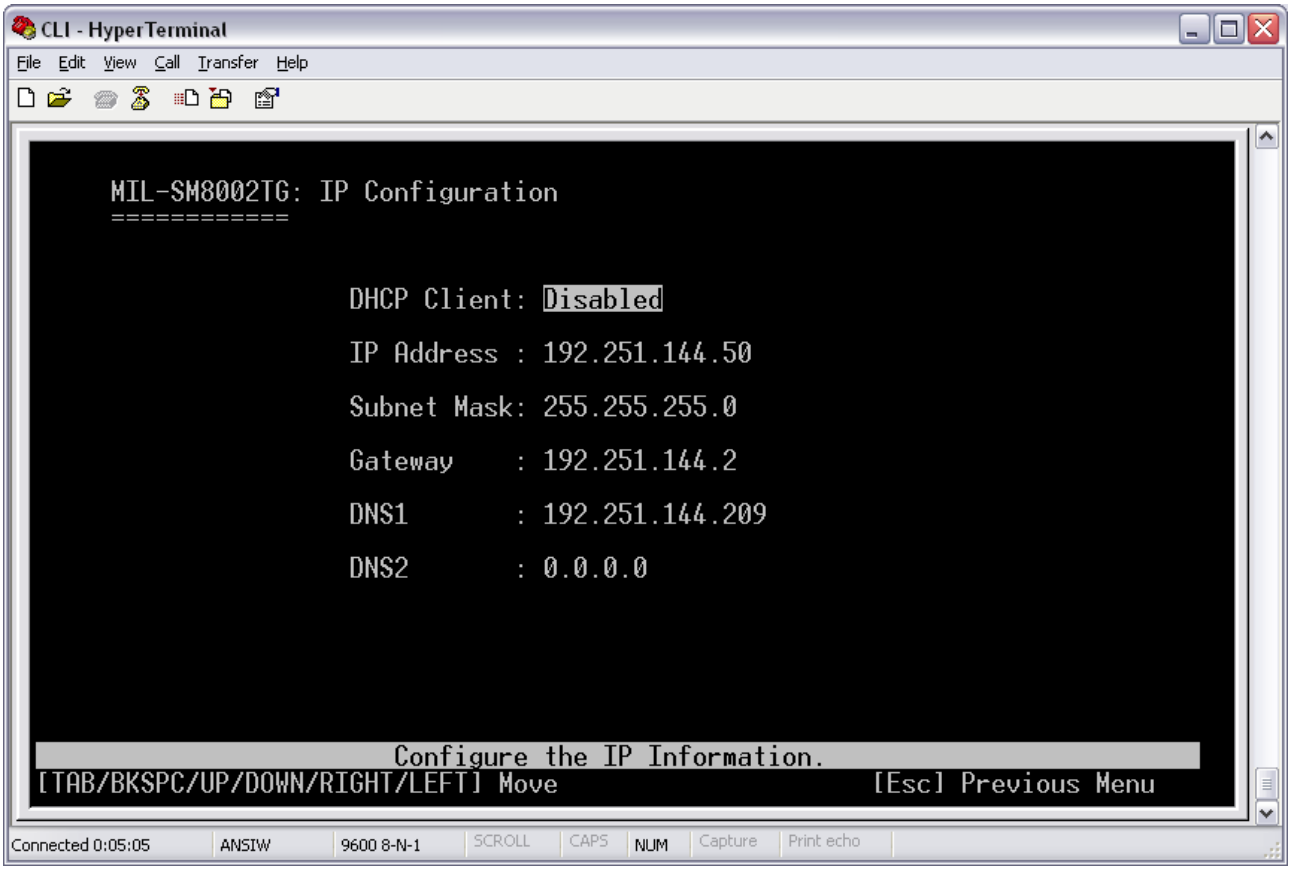
You can configure the IP for the switch. The system has the default IP address. You can re-configure or use the default value.

1. **DHCP:** disable or enable the DHCP client function. When DHCP function is enabling, you don't need to assign the IP address and subnet mask. The system will be assigned the IP address from the local DHCP server.
2. **IP Address:** assign the switch IP address. The default IP is 192.168.1.77
3. **Subnet Mask:** assign the switch IP subnet mask.
4. **Gateway:** assign the switch gateway. The default value is 192.168.1.254
5. **DNS1:** Short for Domain Name Server an Internet service that translates domain

name into IP addresses. Because domain name are alphabetic, they're easier to remember. The Internet is based on IP address. Every time you use a domain name , therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name **www.net.com** might translate to **192.168.1.1**.

6. **DNS2:** The backup for DNS1. When the DNS1 cannot function, the DNS2 can replace DNS1 immediately.
7. Select **<Save>** action to save the configuration.

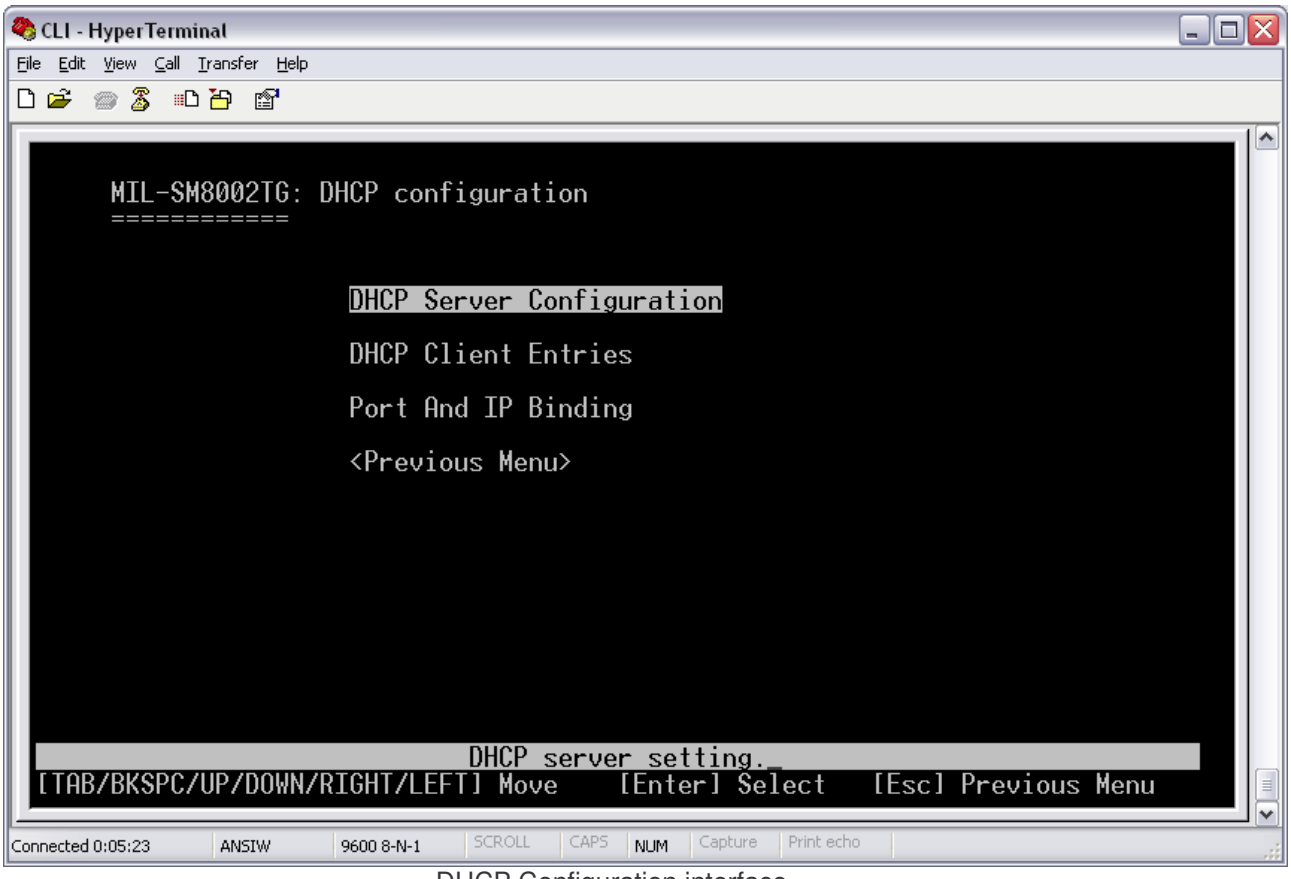
[NOTE] Always restart the switch after finished the setup.



IP Configuration interface

DHCP Configuration

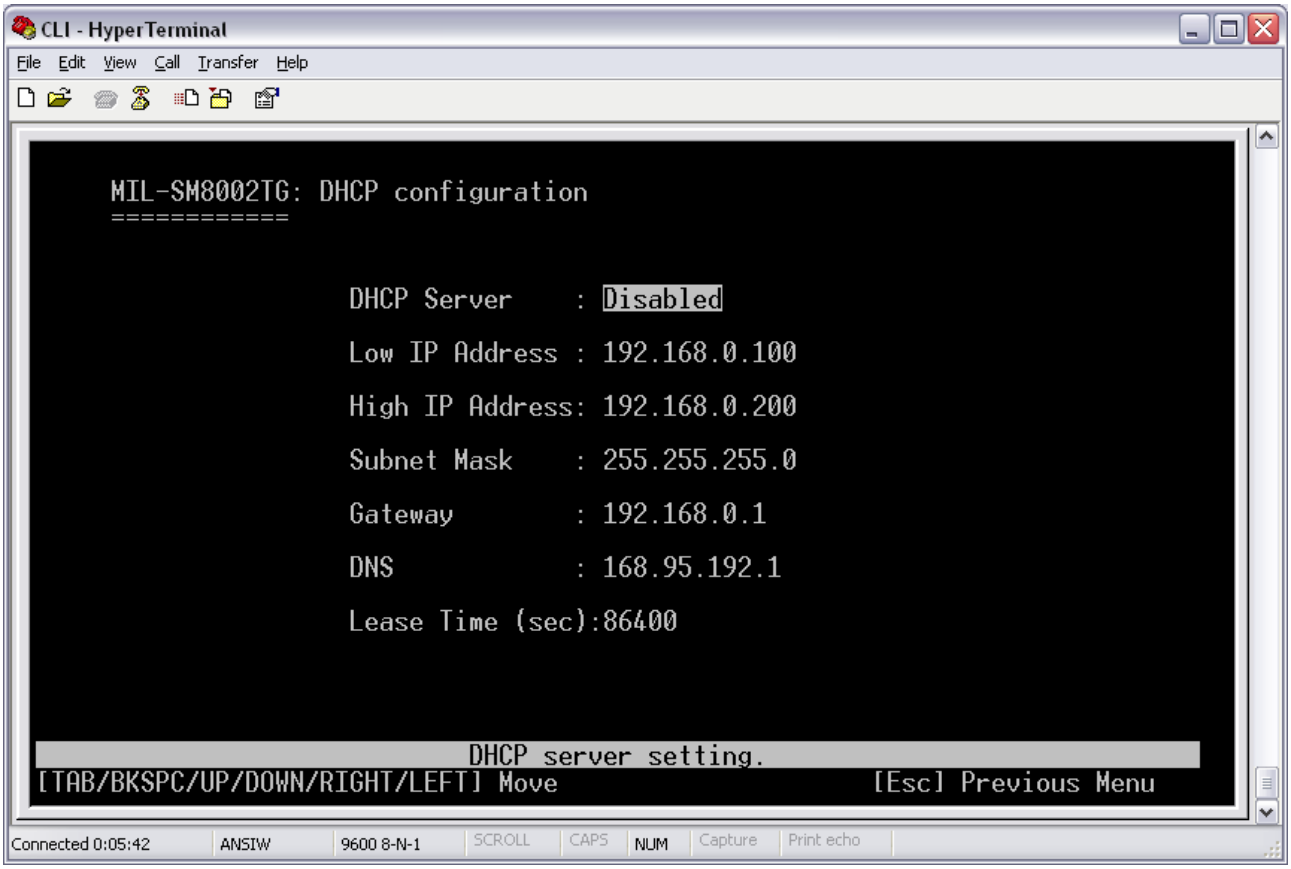
It short for Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: DHCP configuration
DHCP Server Configuration
DHCP Client Entries
Port And IP Binding
<Previous Menu>
DHCP server setting._
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:05:23 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
DHCP Configuration interface

DHCP Server Configuration

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

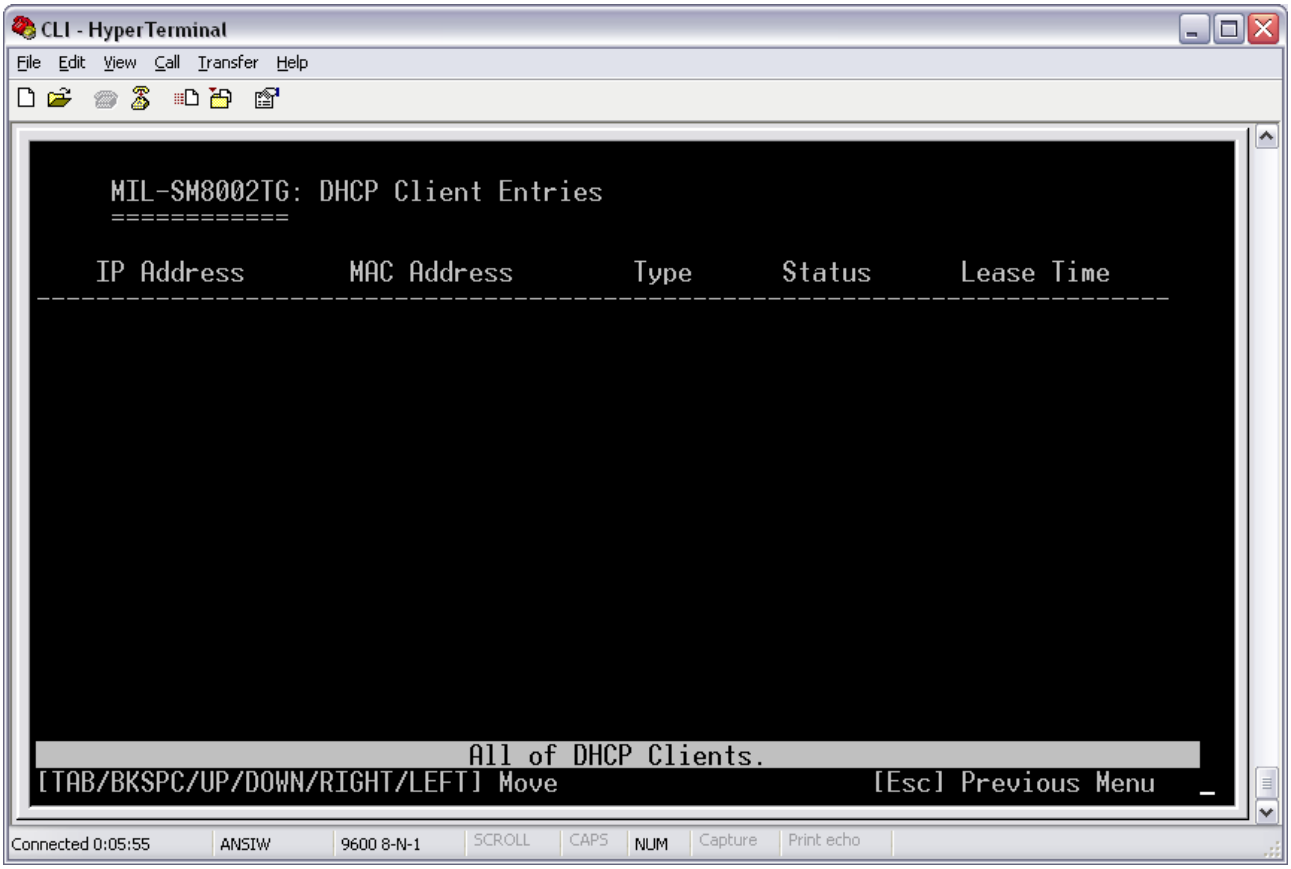
- **DHCP Server:** Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network.
- **Low IP Address:** the dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.169.1.0 ~ 192.168.1.30. 192.168.1.0 will be the Low IP address.
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.169.1.0 ~ 192.168.1.30. 192.168.1.30 will be the High IP address.
- **Subnet Mask:** the dynamic IP assign range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.



DHCP Server Configuration interface

DHCP Client Entries

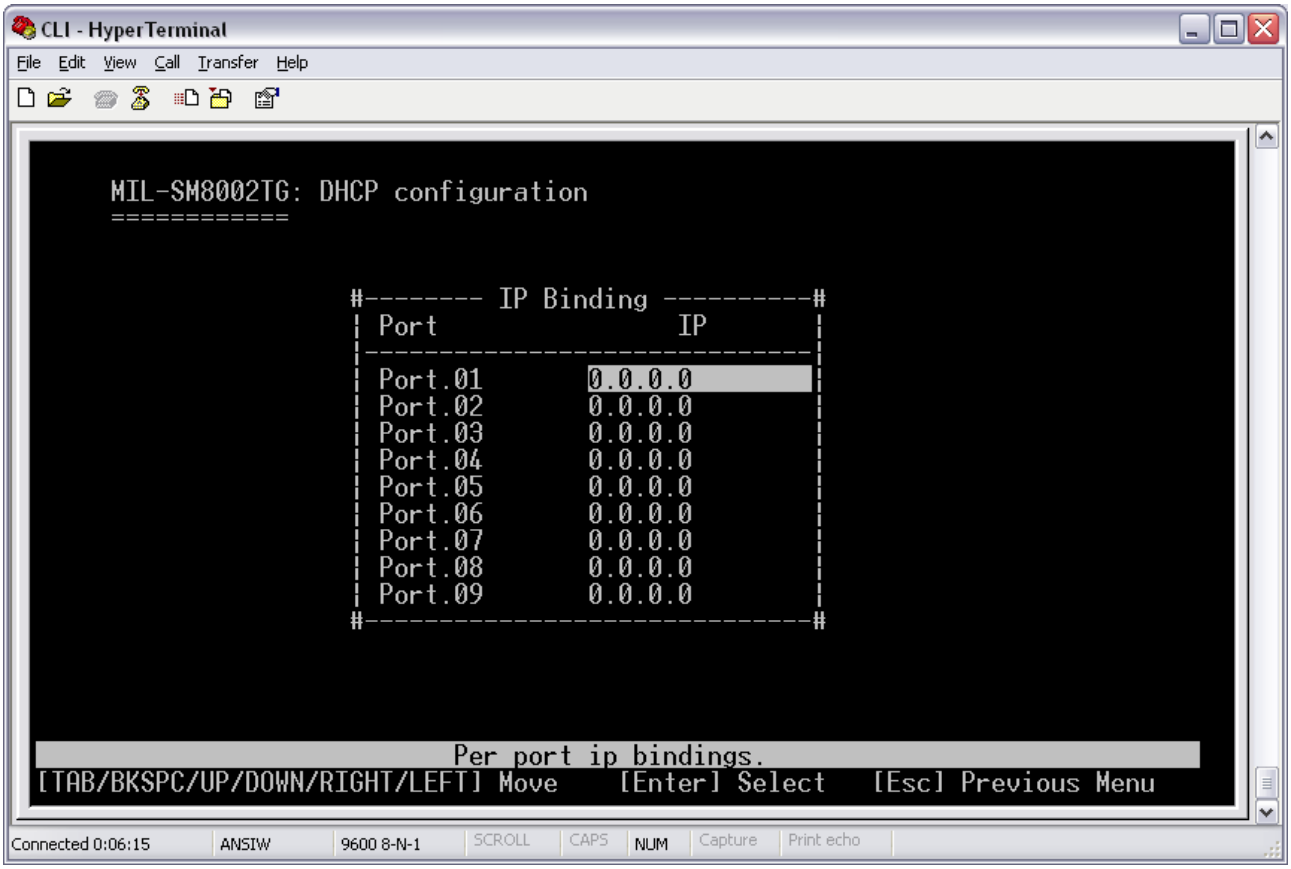
When the DHCP server function is active, the system will collect the DHCP client information and display in here.



DHCP Client Entries interface

Port and IP Bindings

You can assign the specific IP address that is the IP in dynamic IP assign range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before to the connected device.



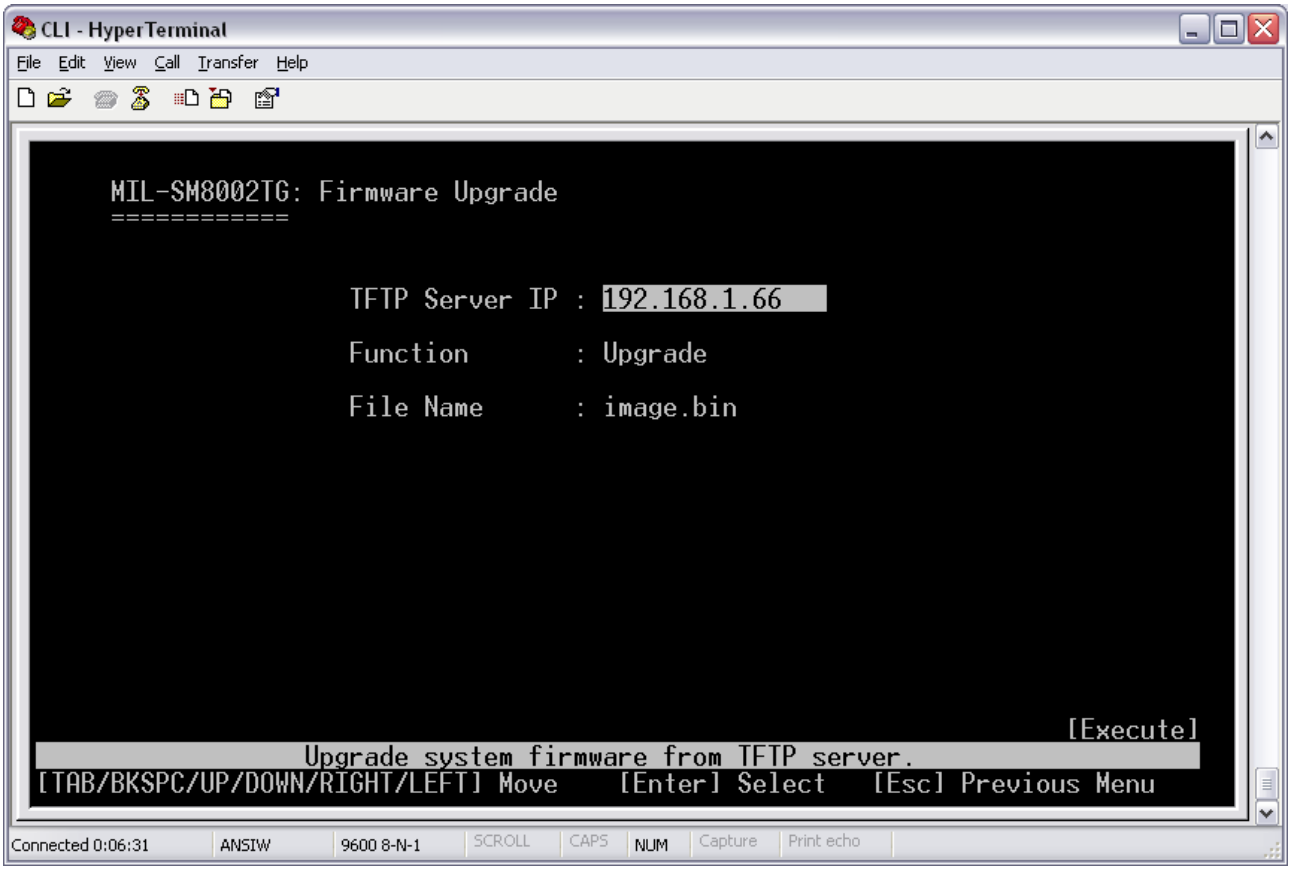
Port and IP Bindings interface

Firmware Update

It provides user to update firmware or restore EEPROM value or backup current EEPROM value.

1. Start the TFTP server, and copy new firmware version image file to the TFTP server.
2. **TFTP Server IP:** type the IP of TFTP server.
3. **Function:** the system provides three functions – update, restore, and backup.
   - **Update:** update the firmware.
   - **Restore:** restore EEPROM value, which saved in TFTP server, from TFTP server.
   - **Backup:** save current EEPROM value to TFTP server as backup. The backup file can be restore from TFTP server when you need.

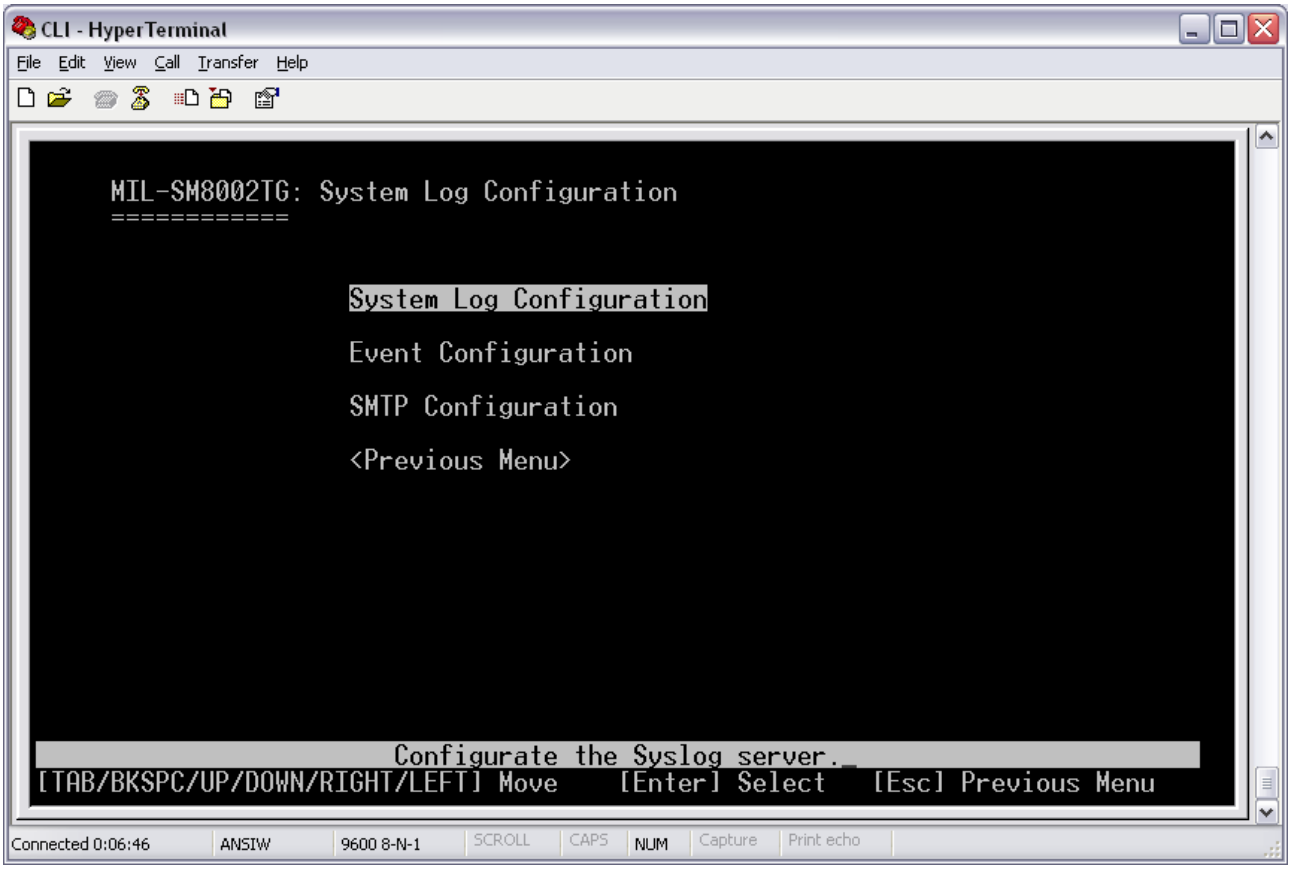
4. **File Name:** type the image file name.
5. Press “**ESC**” to back to action line.
6. “**Save**” the configuration.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Firmware Upgrade
TFTP Server IP : 192.168.1.66
Function : Upgrade
File Name : image.bin
[Execute]
Upgrade system firmware from TFTP server.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:06:31 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Firmware Update interface

System Event Log

You can configure the switch as the system log client that can view the system log information that from the system log server that you have assigned.

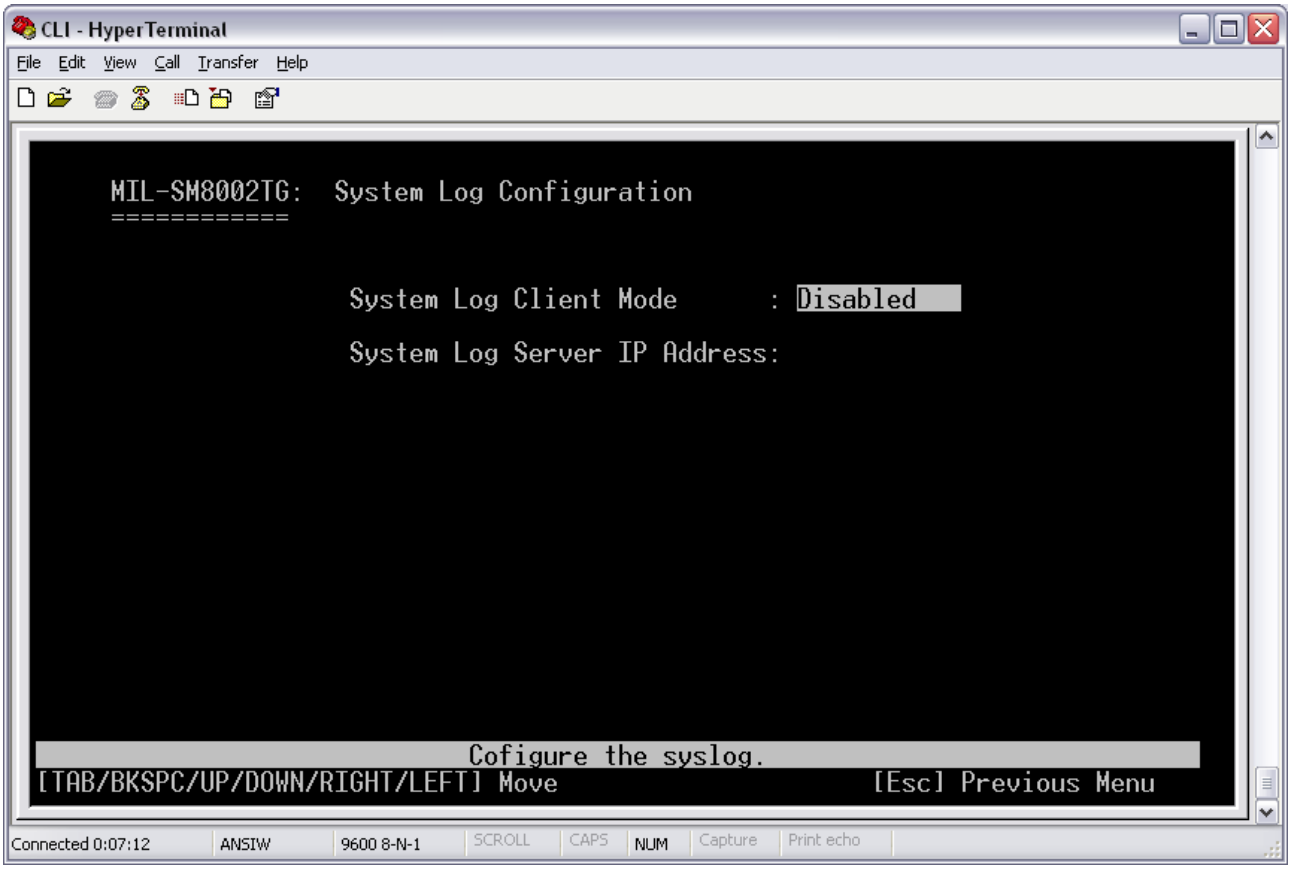

CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: System Log Configuration
System Log Configuration
Event Configuration
SMTP Configuration
<Previous Menu>
Configurate the Syslog server.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:06:46 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

System Log Configuration interface

System Log Configuration

Configuring the system event mode that want to be collected and system log server IP.

1. **Collection Mode:** select the system log mode – client only, server only, or both S/C.
2. **System Log Server IP Address:** assigned the system log server IP.

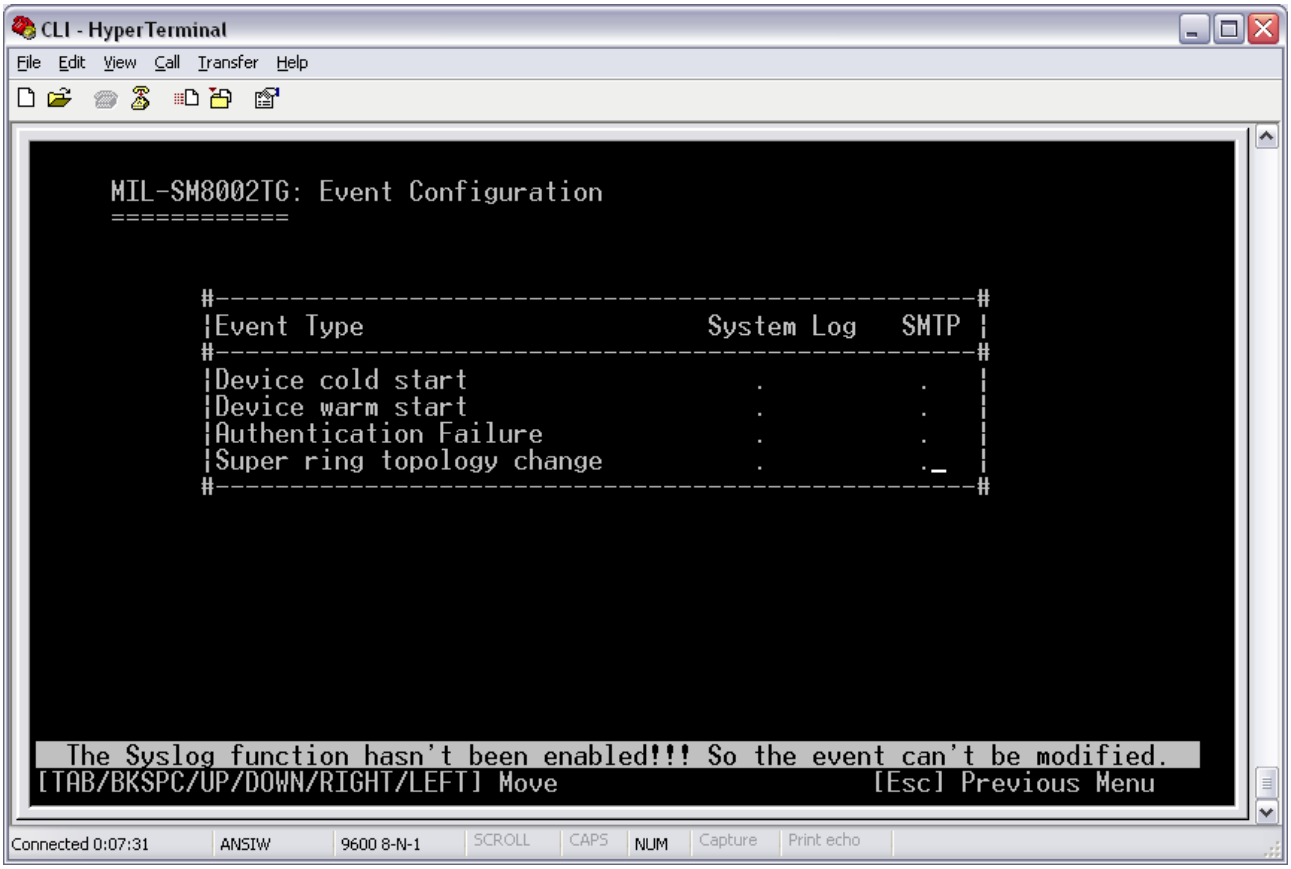


System Log Configuration interface

Event Configuration

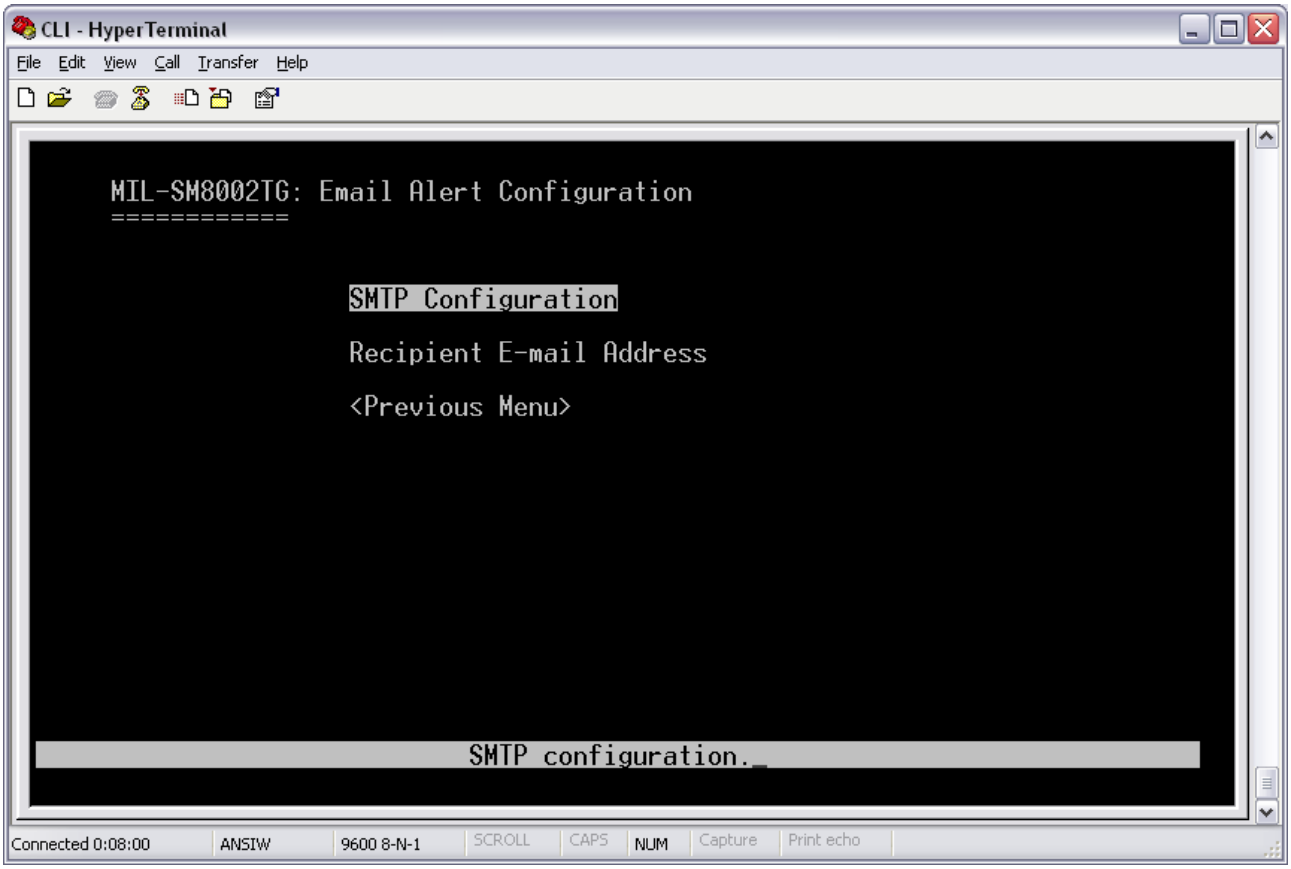
You can select the system log and SMTP events. When selected events occur, the system will send out the log information or alert.

- **Device cold start:** when the device executes cold start action, the system will produce a log event.
- **Device warm start:** when the device executes warm start, the system will produce a log event.
- **Authentication Failure:** when the SNMP authentication fails, the system will produce a log event.
- **Super Ring topology change:** when the Super ring topology has changed, the system will produce a log event.



Email Alert Configuration

When the specific events occur, the system will send the alert to the email account that is assigned by user.

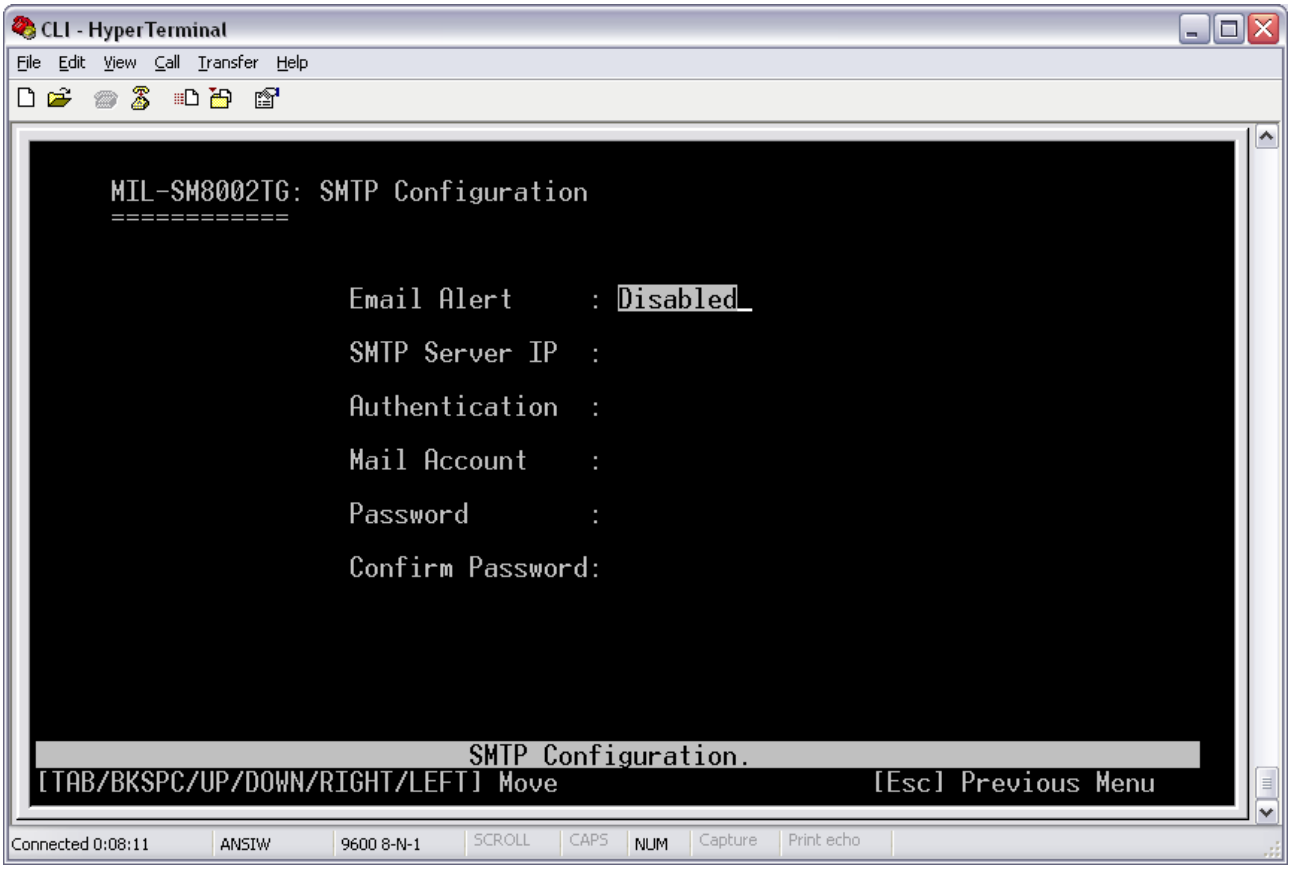


Email Alert Configuration interface

SMTP Configuration

You can set up the mail server IP, mail account, and account password.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address.
3. **Authentication:** mark the check box to enable and configure the email account and password for authentication.
4. **Mail Account:** set up the email account to receive the alert. Ex: johnadmin@123.com. The email account must exist on the mail server, which you had set up in **SMTP Server IP Address** column.
5. **Password:** The email account password.
6. **Confirm Password:** reconfirm the password.

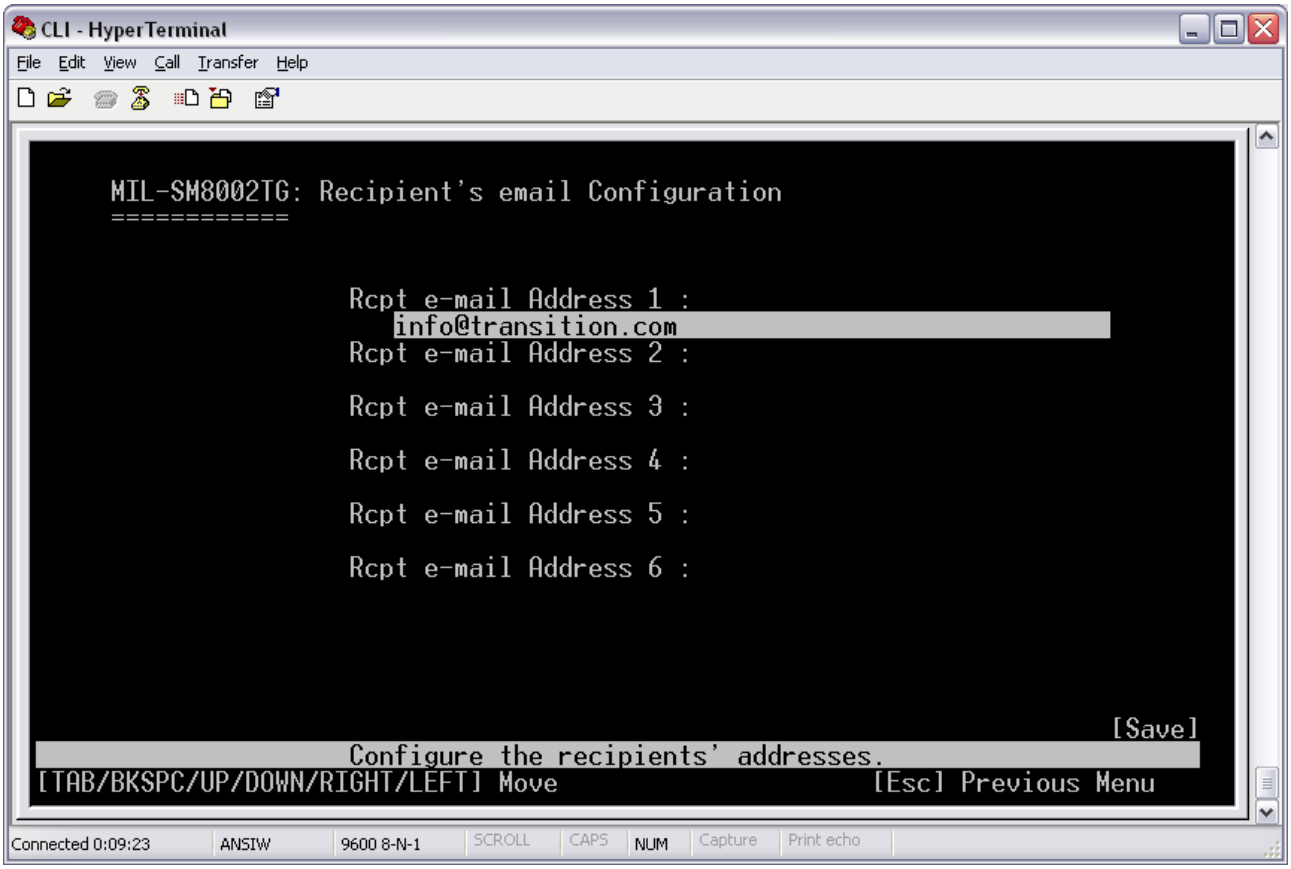


SMTP Configuration interface

Recipient's email Configuration

Assign the forwarded email account for receiving the event alert.

- **Rcpt E-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.

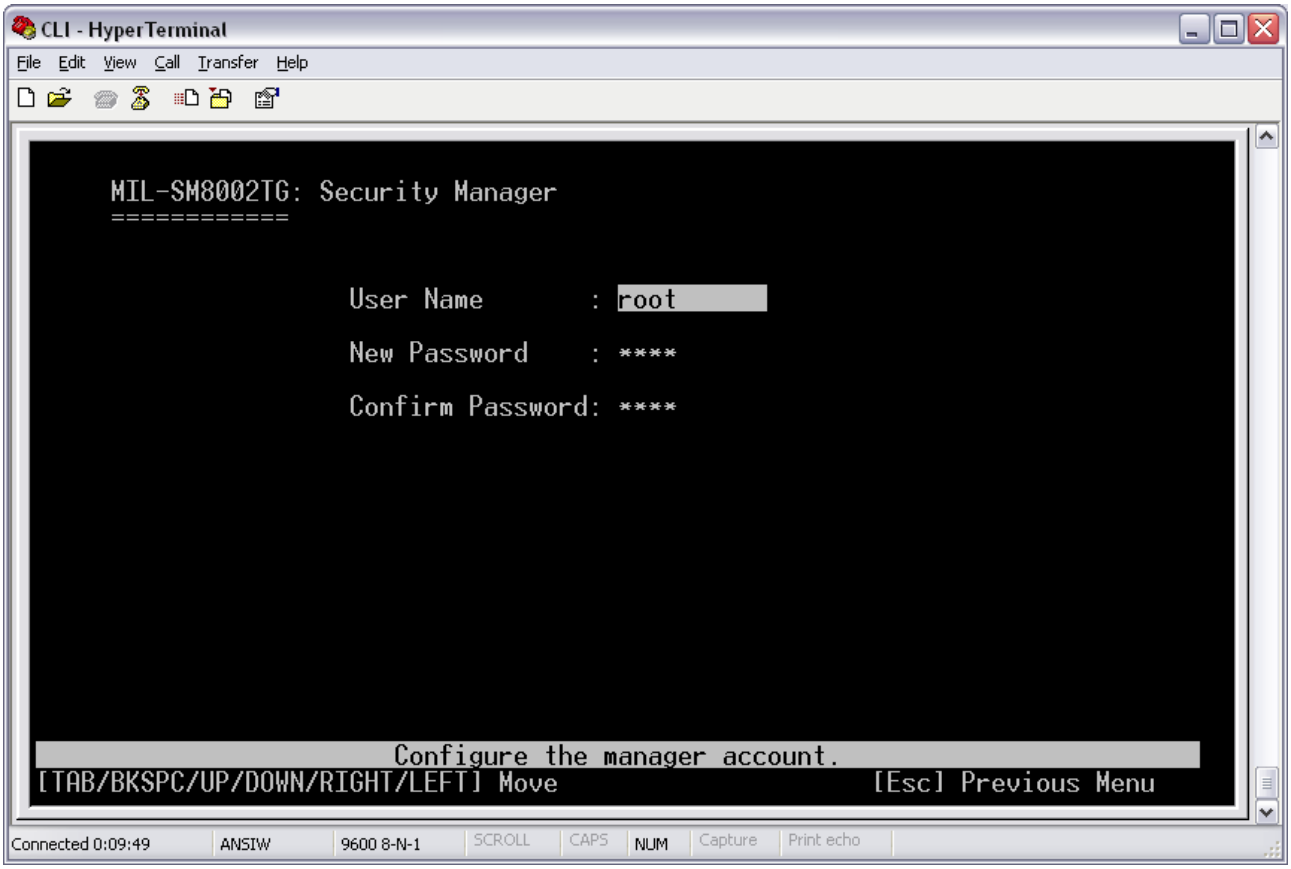


Recipient's email Configuration interface

Security Manager

You can change the console and web management login user name and password for the security issue.

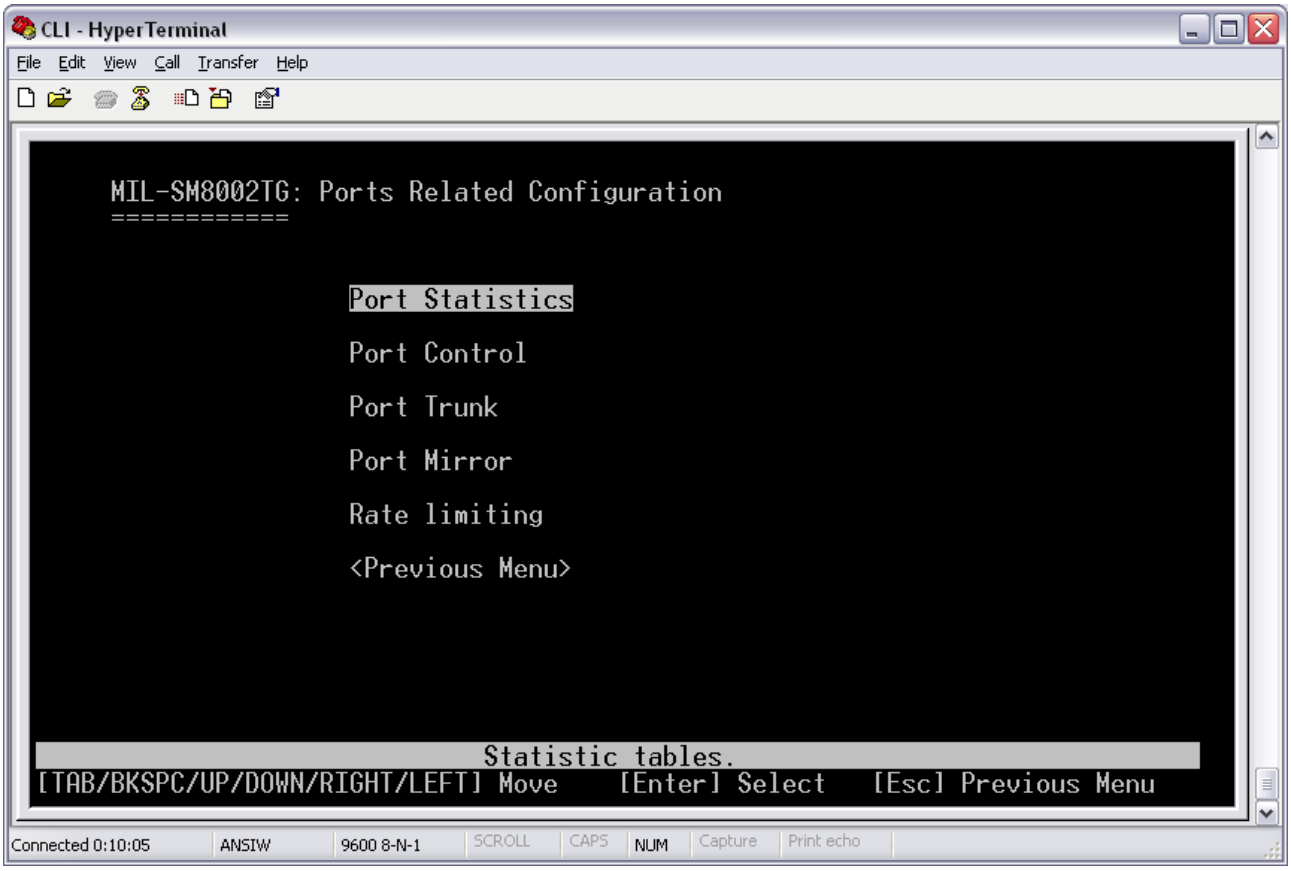
1. **User Name:** Enter the new user name. The default user name is "root".
2. **New Password:** enter the new password. The default password is "root"
3. **Confirm Password:** reenter the new password for confirmation.



Security Manager interface

Port Configuration

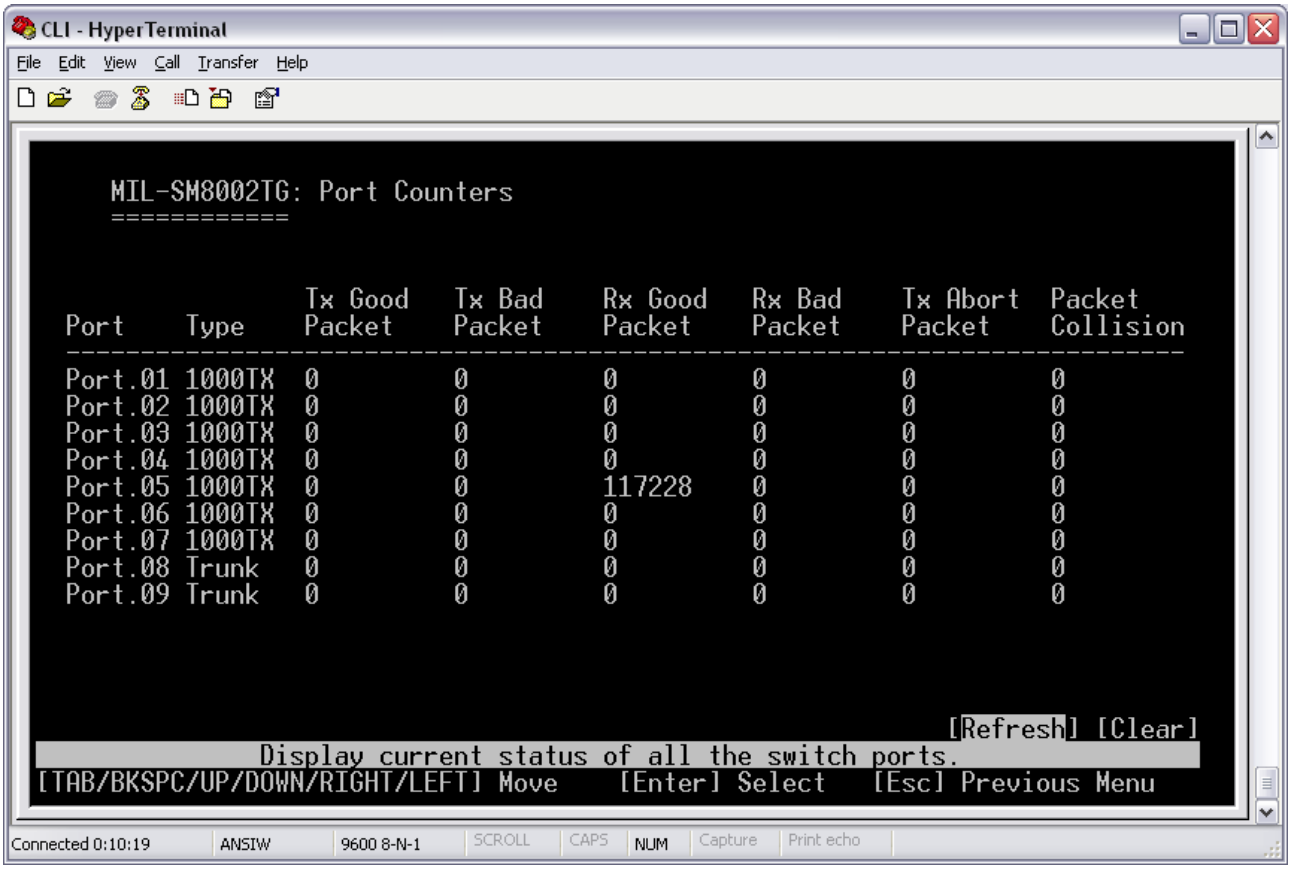
In this section, you can view port counter information; configure port control, mirroring, trunk, and rate limiting.



Port Configuration main interface

Port Counters

It displays the current port counter information. Select the **<Refresh>**action to get newest port counter information. Select the **<Clear>** action to set the port counter information back to 0.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Port Counters
Port Type Tx Good Packet Tx Bad Packet Rx Good Packet Rx Bad Packet Tx Abort Packet Packet Collision
Port.01 1000TX 0 0 0 0 0 0
Port.02 1000TX 0 0 0 0 0 0
Port.03 1000TX 0 0 0 0 0 0
Port.04 1000TX 0 0 0 0 0 0
Port.05 1000TX 0 0 117228 0 0 0
Port.06 1000TX 0 0 0 0 0 0
Port.07 1000TX 0 0 0 0 0 0
Port.08 Trunk 0 0 0 0 0 0
Port.09 Trunk 0 0 0 0 0 0
[Refresh] [Clear]
Display current status of all the switch ports.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:10:19 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

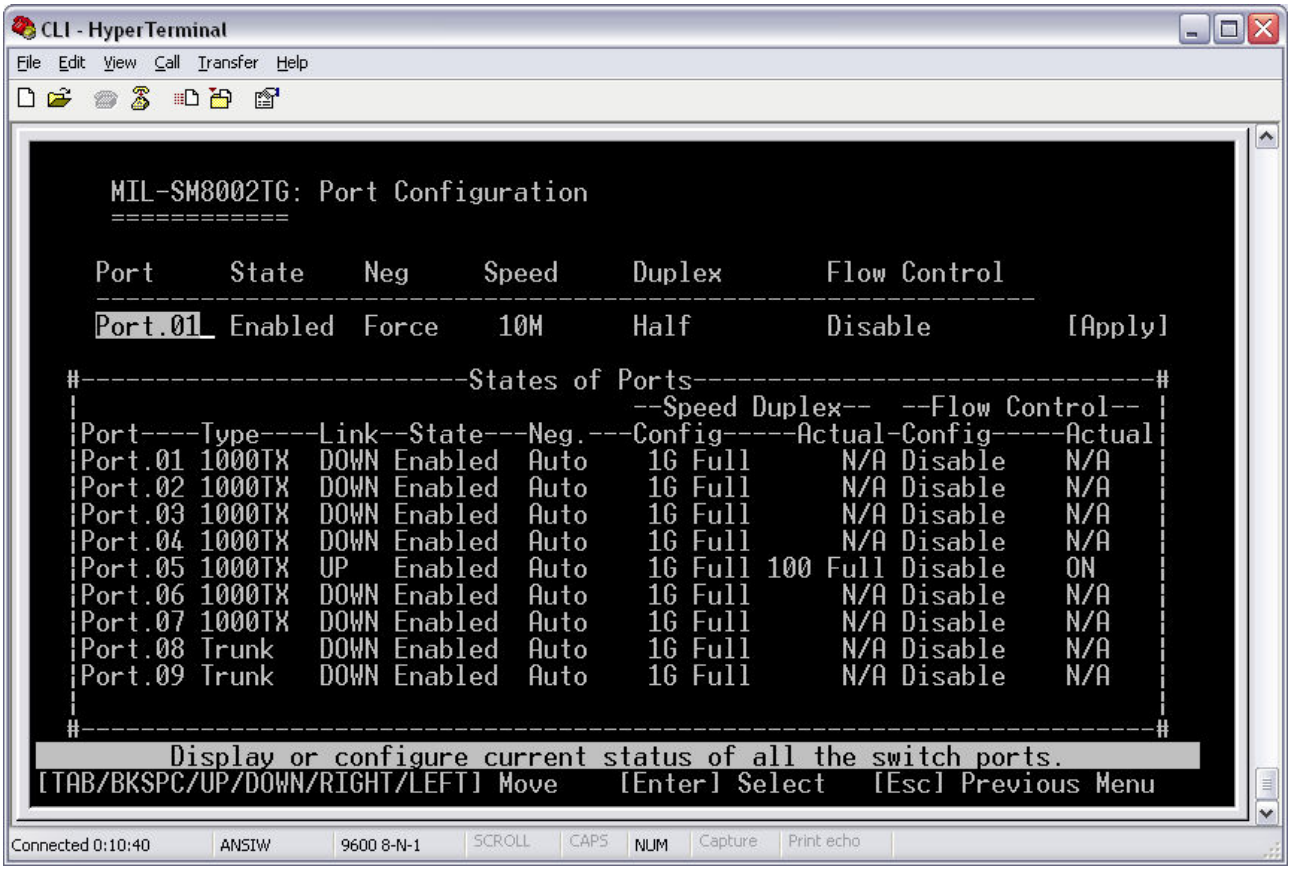
Port Counter interface

Port Control Configuration

You can set up every port status.

1. Use “**Tab**” key to move between items.
2. **Port:** select the port that wants to be configured.
3. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
4. **Neg:** set auto negotiation status of port.
5. **Speed:** set the port link speed.
6. **Duplex:** set full-duplex or half-duplex mode of the port.
7. **Flow Control:** enable or disable Flow control function (Flow control is for full duplex link mode).
8. Select the **<Save>**.

9. To view the **State of Ports**, select **<Refresh>** to get the current ports state information.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Port Configuration
Port State Neg Speed Duplex Flow Control
Port.01 Enabled Force 10M Half Disable [Apply]
States of Ports
--Speed Duplex-- --Flow Control--
Port----Type----Link--State---Neg.---Config-----Actual-Config-----Actual
Port.01 1000TX DOWN Enabled Auto 1G Full N/A Disable N/A
Port.02 1000TX DOWN Enabled Auto 1G Full N/A Disable N/A
Port.03 1000TX DOWN Enabled Auto 1G Full N/A Disable N/A
Port.04 1000TX DOWN Enabled Auto 1G Full N/A Disable N/A
Port.05 1000TX UP Enabled Auto 1G Full 100 Full Disable ON
Port.06 1000TX DOWN Enabled Auto 1G Full N/A Disable N/A
Port.07 1000TX DOWN Enabled Auto 1G Full N/A Disable N/A
Port.08 Trunk DOWN Enabled Auto 1G Full N/A Disable N/A
Port.09 Trunk DOWN Enabled Auto 1G Full N/A Disable N/A
Display or configure current status of all the switch ports.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:10:40 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Port Control Configuration interface

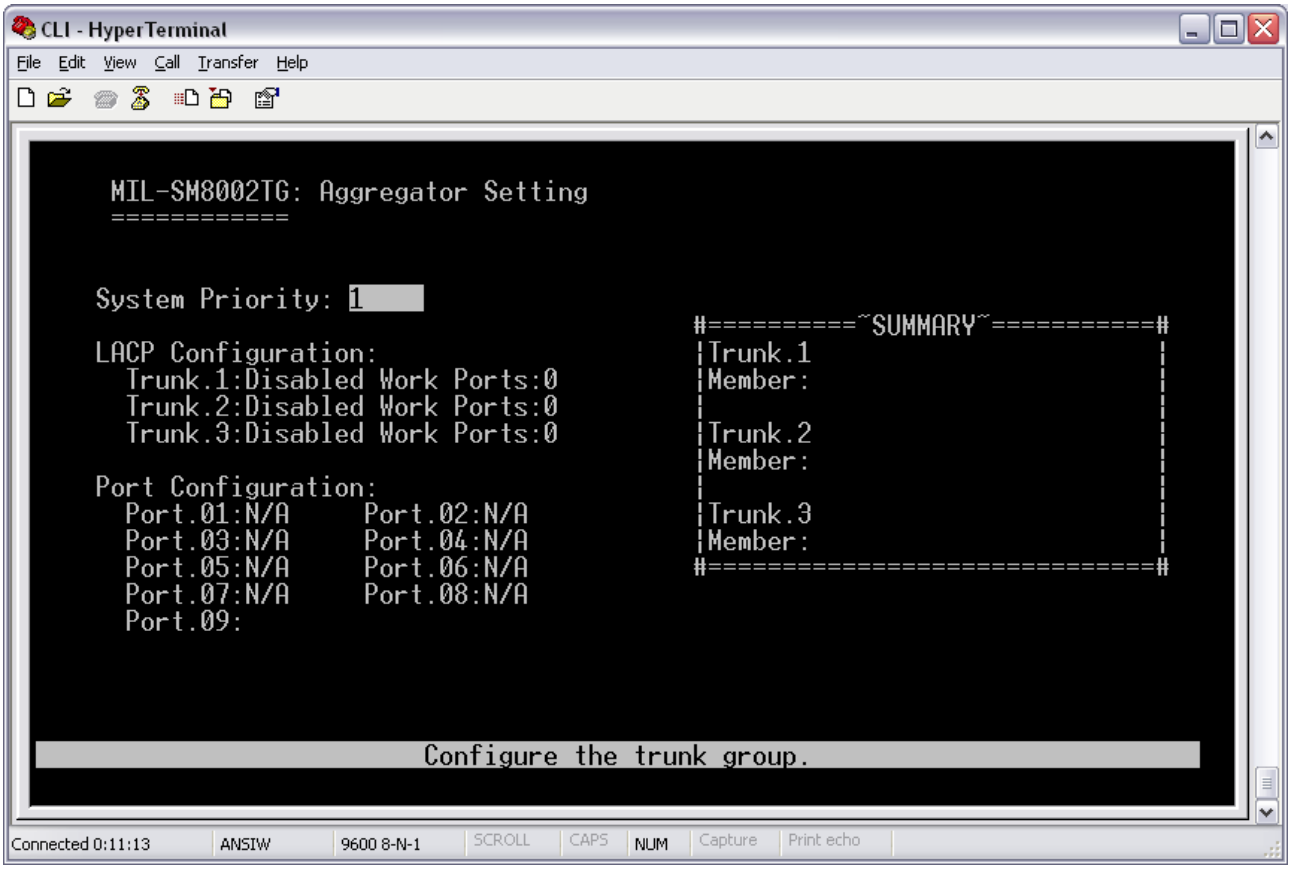
Trunk Configuration

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to nine consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex**

mode, more detail information refers to IEEE 802.3ad.

Aggregator setting

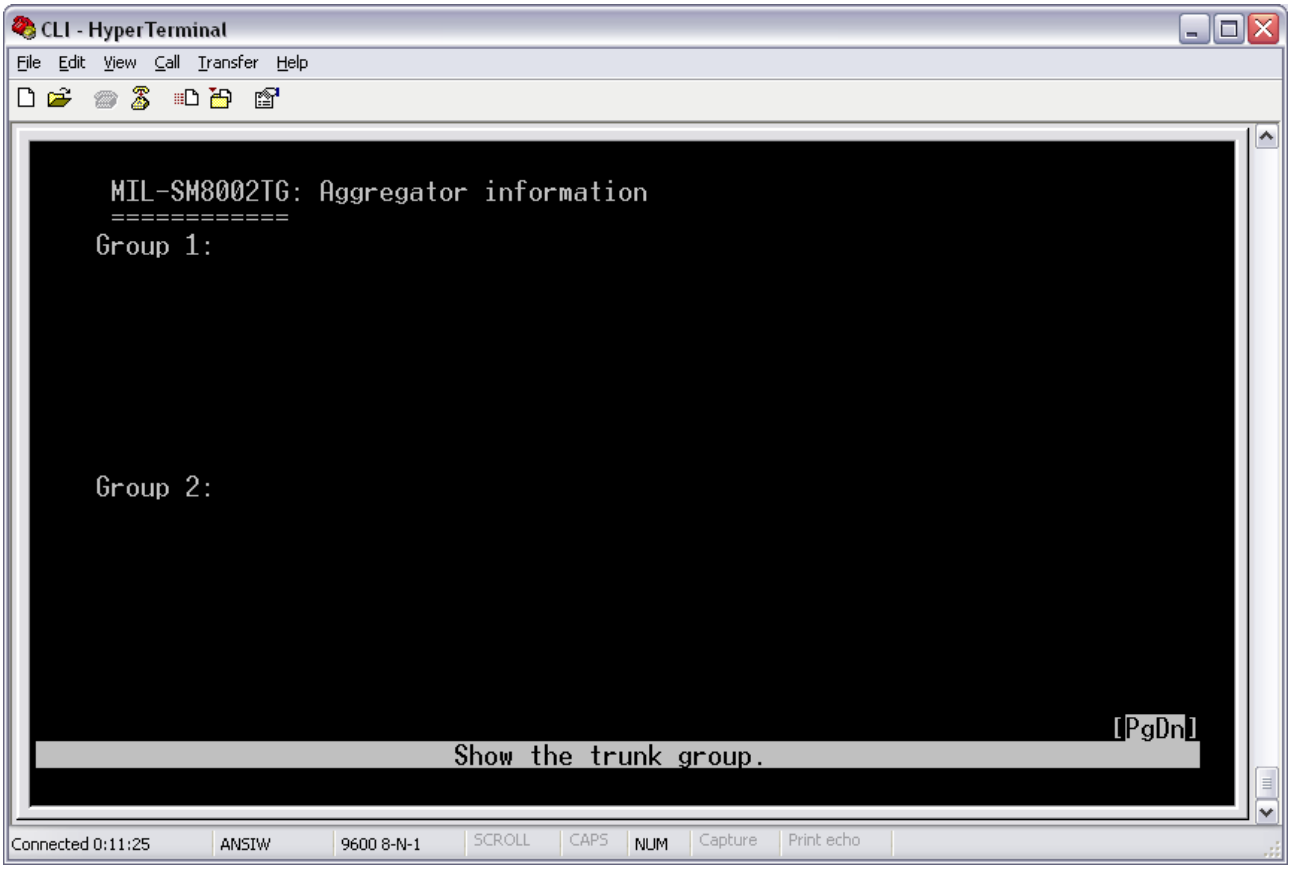
1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **LACP Configuration:** If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
   - **Trunk Group:** there are three-trunk group – trunk 1, 2, and 3. You can select the trunk group and enable the LACP or disable it.
   - **Work ports:** select a work port number for the trunk group. The LACP static trunk group work port number cannot be 0.
   - **Port Configuration:** to assign the port to the trunk group.
3. Select the ports to join the trunk group.
4. Select the **<Save>** to save the configuration.
5. You can view the setting information in summary frame.



Trunk Configuration — Aggregator Setting interface

Aggregator Information

When you had setup the LACP aggregator, you will see relate information in here.



Trunk Configuration – Aggregator Information interface

State Activity

When you had setup the LACP aggregator, you can configure port state activity. You can change the port state activity to **Active** or **Passive**.

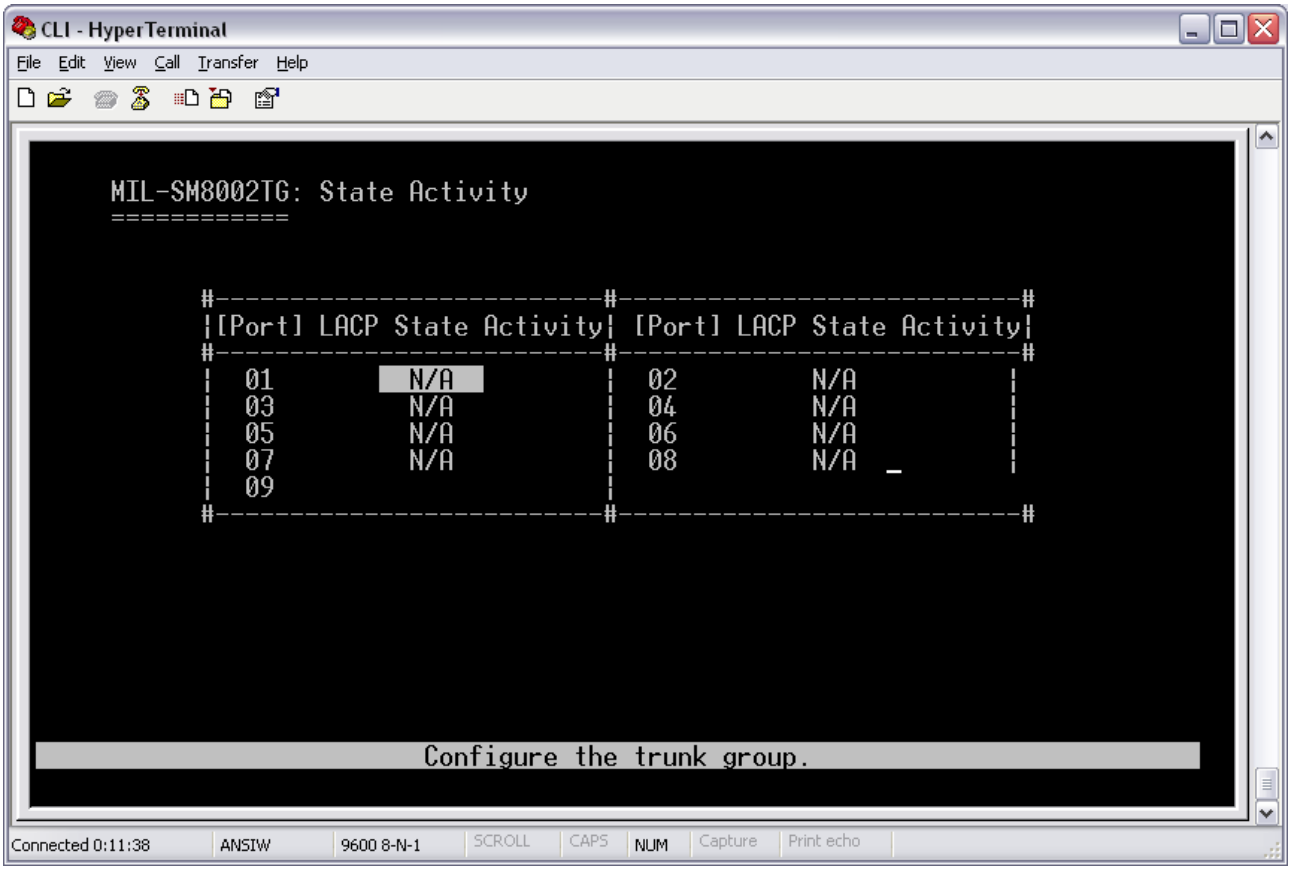
1. **Active:** The port automatically sends LACP protocol packets.
2. **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

a. A link having either two active LACP ports or one active port can perform dynamic LACP trunking.

b. A link has two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for and LACP protocol packet from the opposite device.

c. If you are active LACP's actor, when you are select trunking port, the active status will be created automatically.



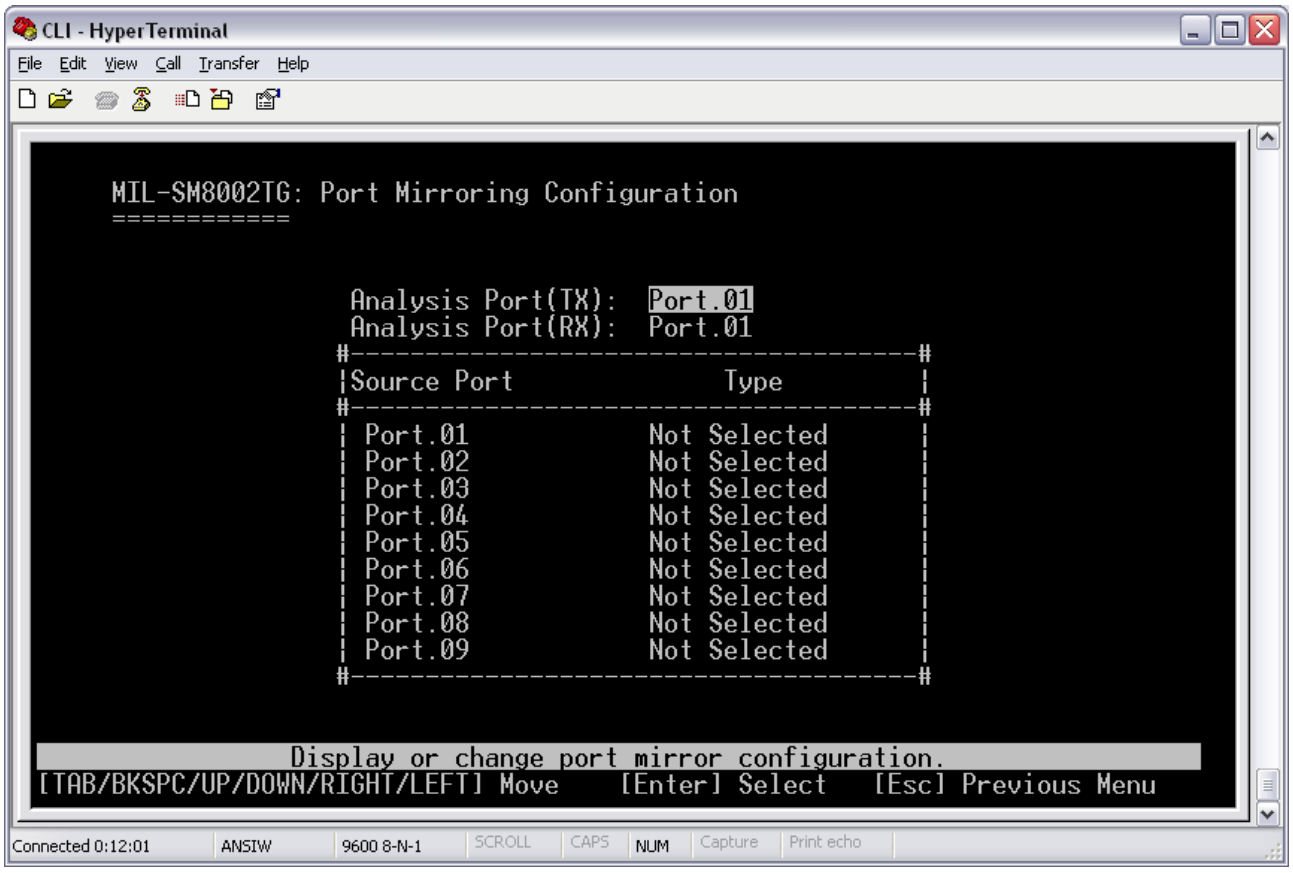
Trunk Configuration – State Activity

Port Mirroring Configuration

The port mirroring is a method for monitor traffic of switched networks. The specific port can monitor traffic through the mirror ports. The monitored ports in or out traffic will be duplicated into monitoring port.

1. **Analysis Port (TX):** It's mean mirror port can be used to see all monitor port traffic. You can connect mirror port to LAN analyzer or Netxray.
2. **Analysis Port (RX):** Set the destination port of mirroring packet. All of the packets of mirroring port will be duplicated and sent to Analysis port.

3. **Source Port (TX/RX)**: select the monitor mode of each port. You can choose which port wants to monitor in only one mirror mode.
   - **RX:** RX packet only
   - **TX:** TX packet only
   - **Both:** RX and TX packet


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Port Mirroring Configuration
Analysis Port(TX): Port.01
Analysis Port(RX): Port.01
Source Port Type
Port.01 Not Selected
Port.02 Not Selected
Port.03 Not Selected
Port.04 Not Selected
Port.05 Not Selected
Port.06 Not Selected
Port.07 Not Selected
Port.08 Not Selected
Port.09 Not Selected
Display or change port mirror configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:12:01 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Port Mirroring interface

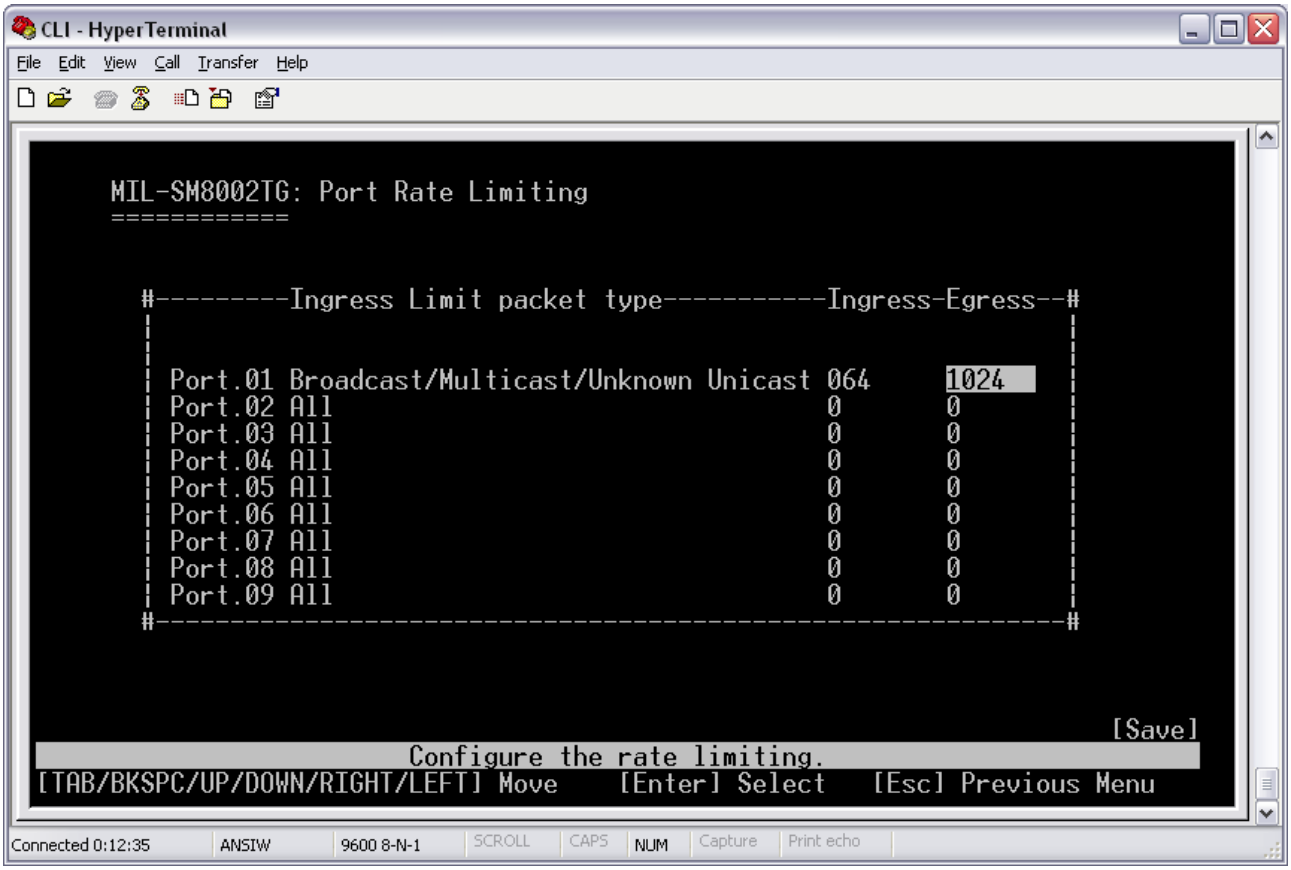
Rate Limiting

You can set up every port's bandwidth rate and packet limitation type.

- **Ingress Limit Packet type:** select the packet type that want to filter. The packet types have all type packet, broadcast/multicast/unknown unicast packet, broadcast/multicast packet, and broadcast packet only. The

broadcast/multicast/unknown unicast packet, broadcast/multicast packet, and broadcast packet only are only for ingress packet. The egress rate only supports all type packet.

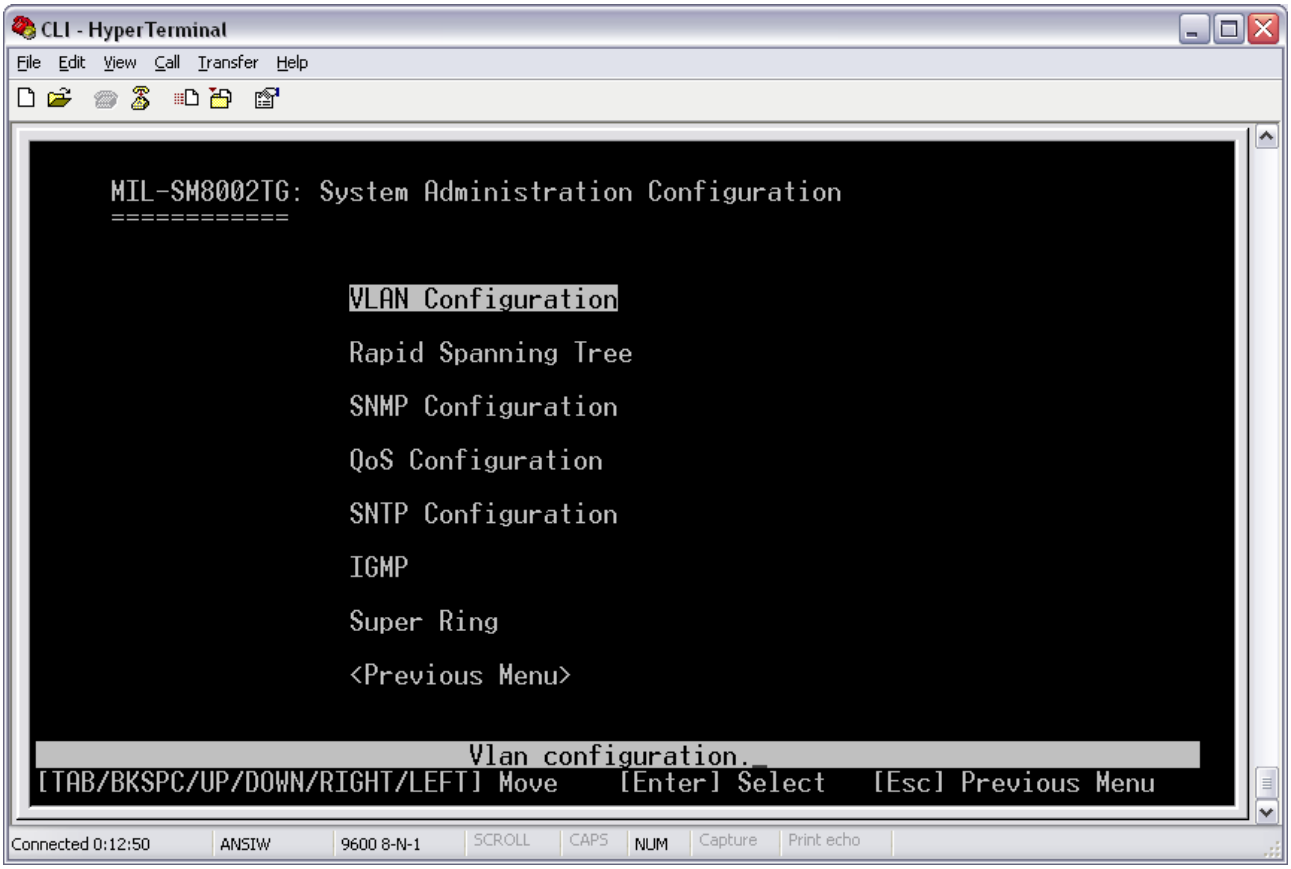
- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate.
  - **Ingress:** enter the port effective ingress rate. The default value is "0".
  - **Egress:** enter the port effective ingress rate. The default value is "0".


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Port Rate Limiting
Ingress Limit packet type
Ingress
Egress
Port.01 Broadcast/Multicast/Unknown Unicast 064 1024
Port.02 All 0 0
Port.03 All 0 0
Port.04 All 0 0
Port.05 All 0 0
Port.06 All 0 0
Port.07 All 0 0
Port.08 All 0 0
Port.09 All 0 0
[Save]
Configure the rate limiting.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:12:35 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Rate Limiting interface

Protocol Configuration

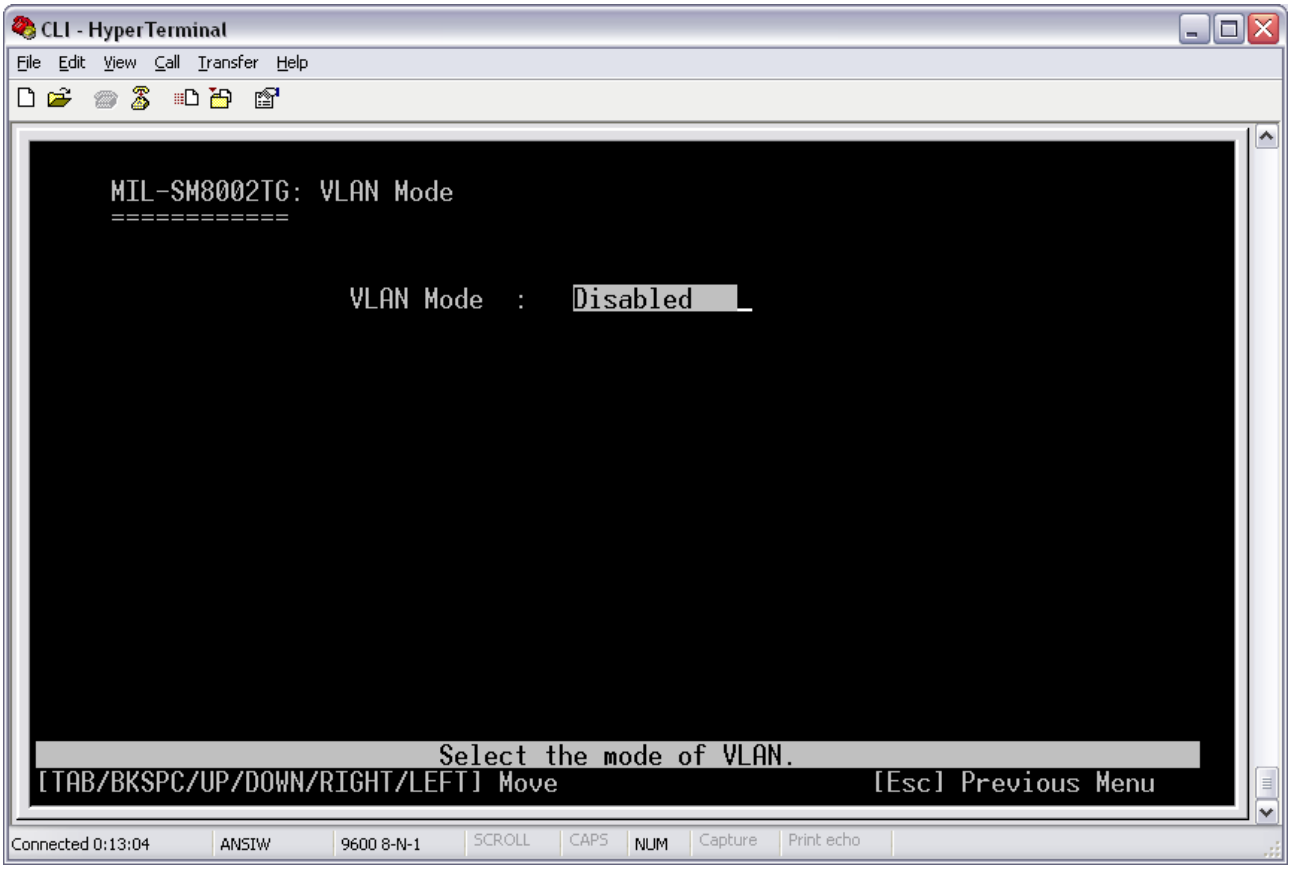
In this section, you can configure VLAN, RST, SNMP, SNTP, QoS, IGMP, and Super ring.



Protocol Configuration interface

VLAN Configuration

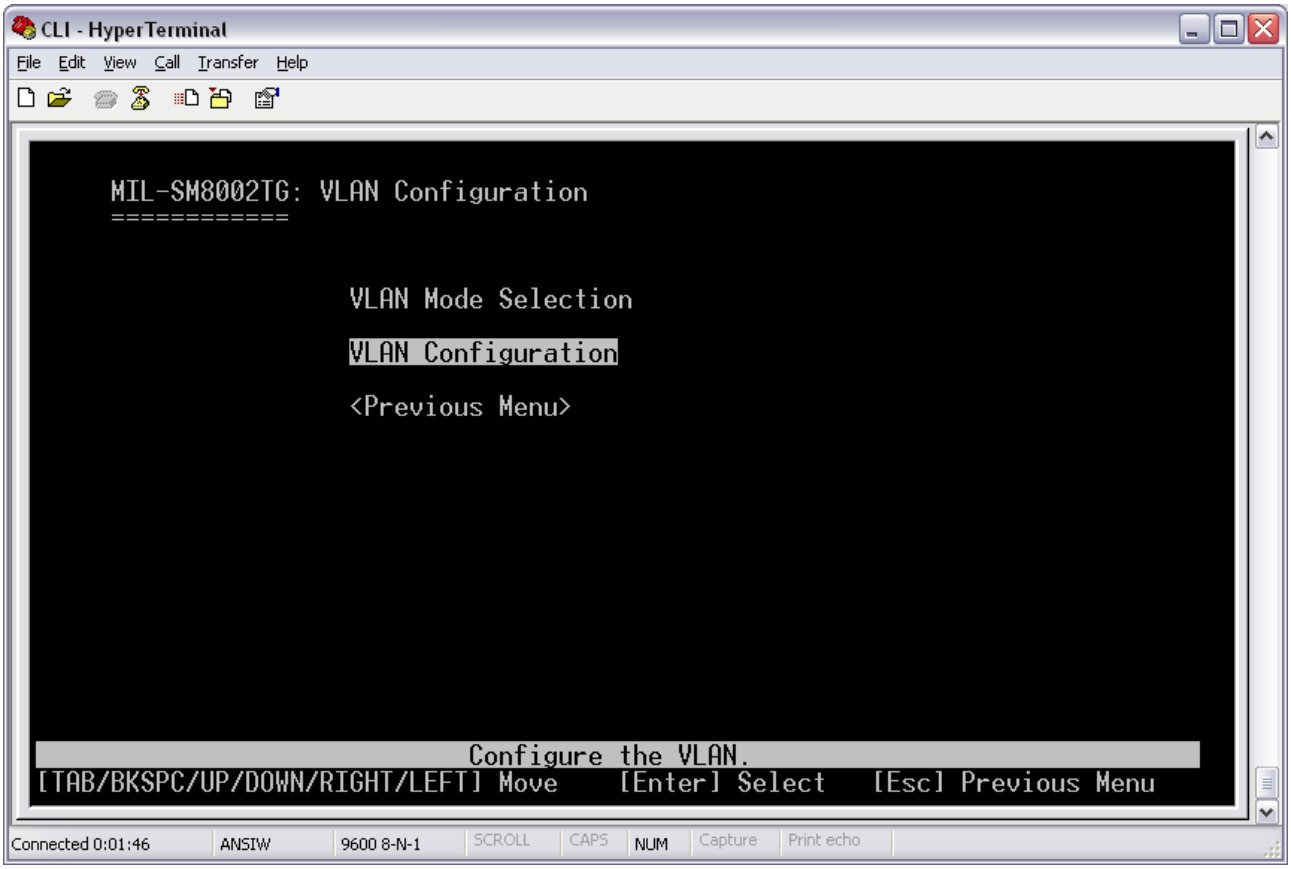
The VLAN Configuration provides two VLAN modes – Port Base and 802.1Q. You need to select the VLAN mode for the VLAN detail configuration. Use **Space** key to switch the VLAN mode selection. After select the VLAN mode, save the selection. Press **ESC** key to exit the VLAN Mode Selection interface.



VLAN Mode Selection interface

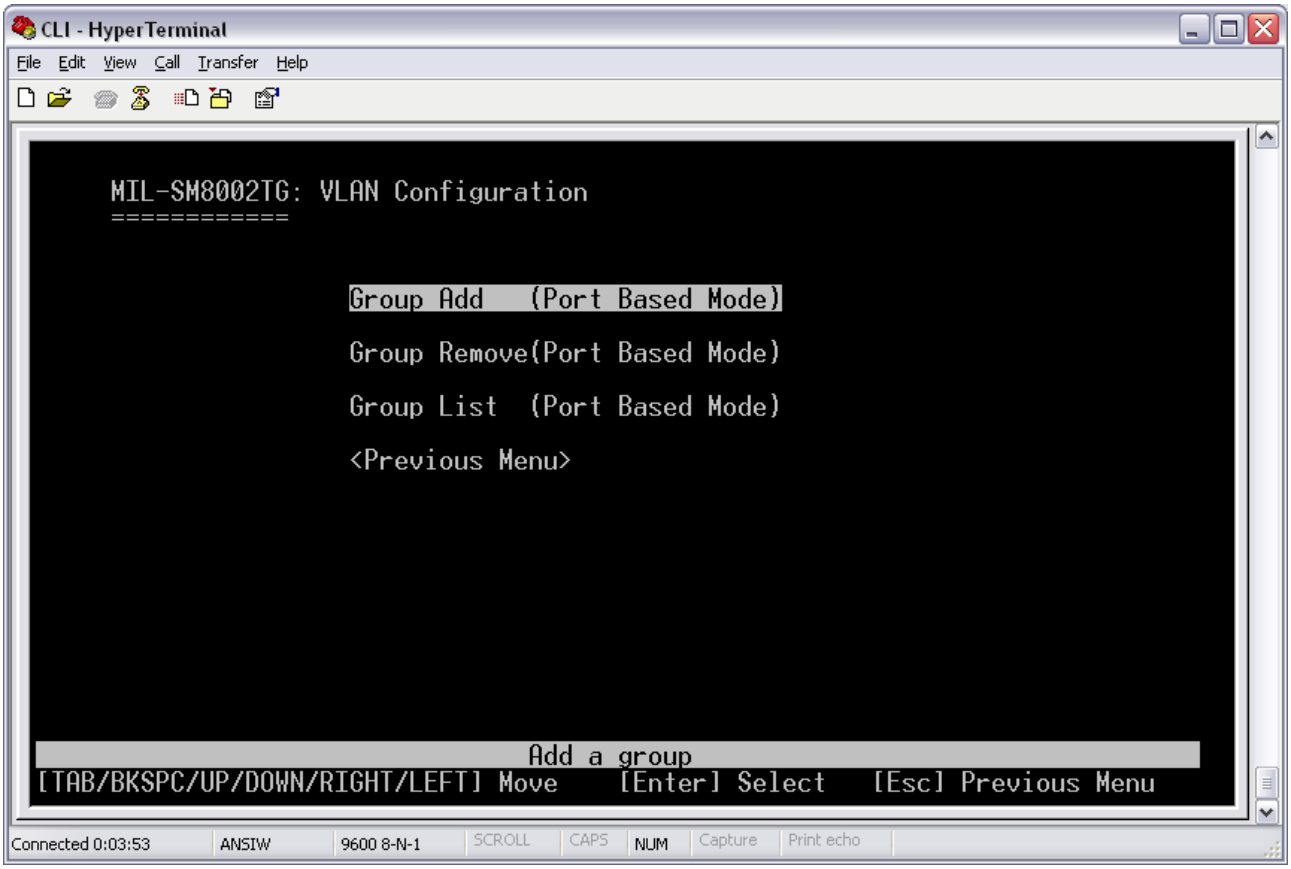
Port Base VLAN Configure

Add VLAN group, remove VLAN group, and view the VLAN group list. Use **Tab** key to move between the configure items.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: VLAN Configuration
VLAN Mode Selection
VLAN Configuration
<Previous Menu>
Configure the VLAN.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:01:46 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Group Add

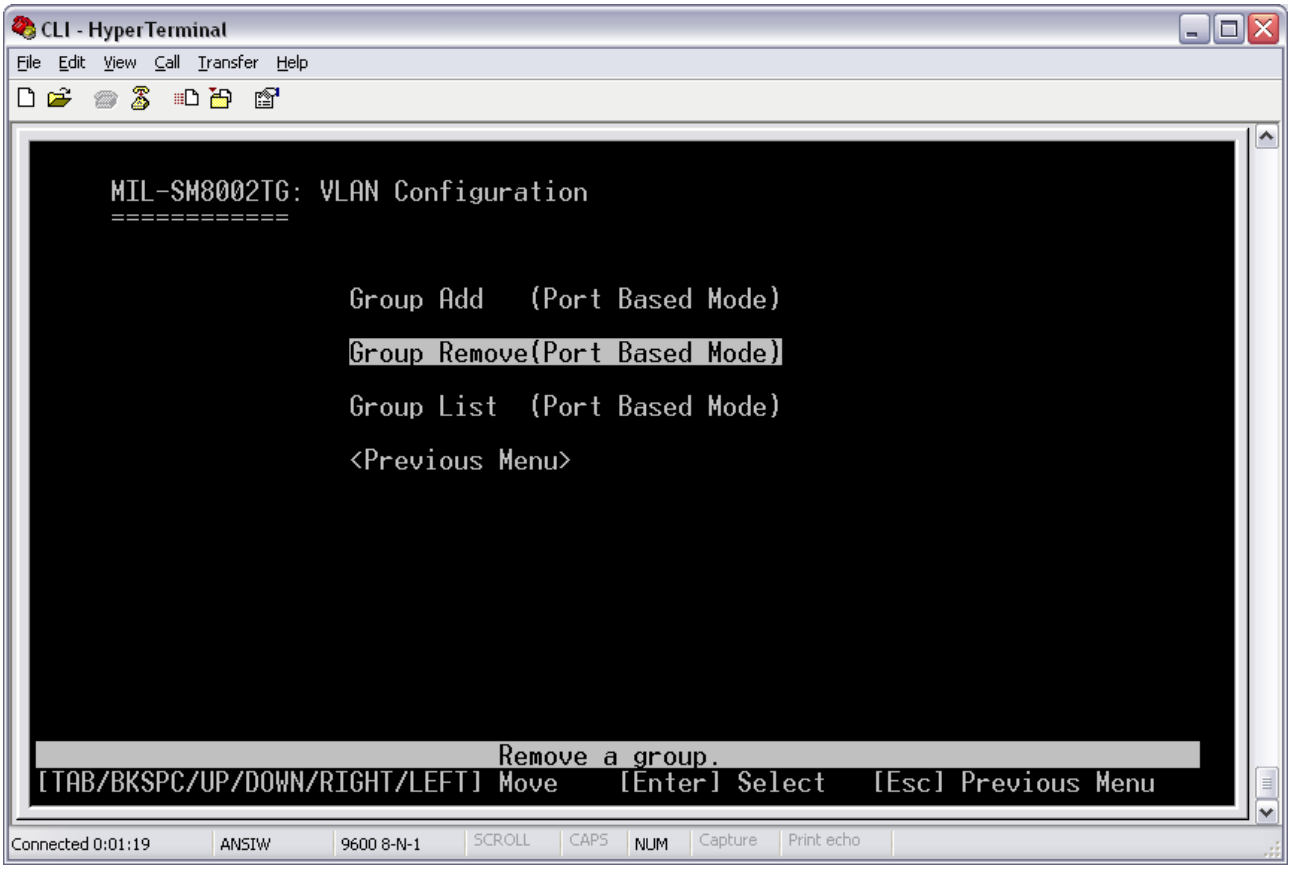
1. **Group Name:** Type a name for the new VLAN, ex: VLAN01.
2. **VID:** Type the VLAN group ID. The group ID rang is from 1 to 4094.
   a. **Member Ports:** Press"**Space**" key to change the port status. Mark the port to be the member..
3. Select **<Save>** to save the configuration.
4. Press **"ESC"** key to go back action menu line.



Group Add interface

Group Remove

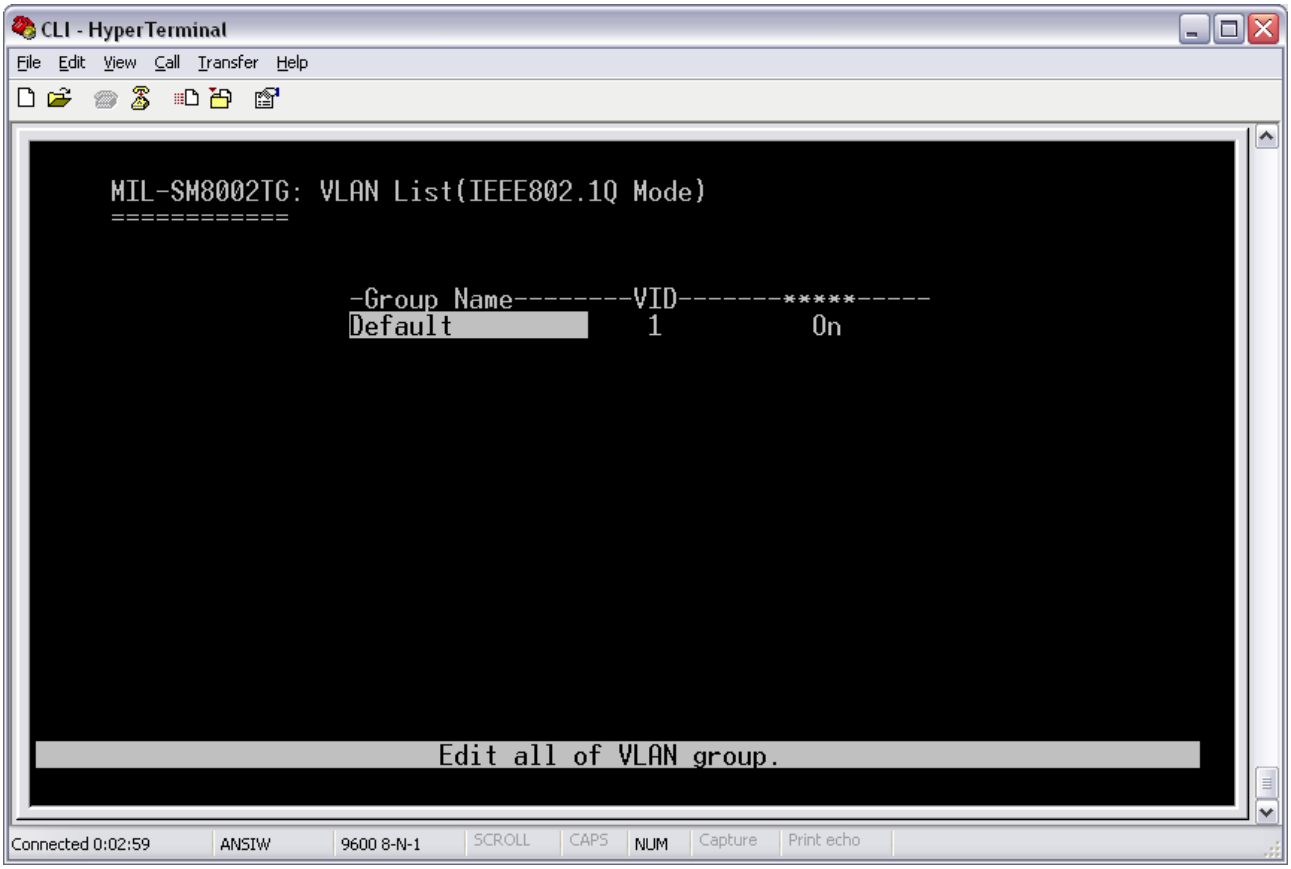
You can remove unwanted VLAN group. Enter the group VID and select **Save**.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: VLAN Configuration
Group Add (Port Based Mode)
Group Remove(Port Based Mode)
Group List (Port Based Mode)
<Previous Menu>
Remove a group.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:01:19 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Group Remove interface

Group List

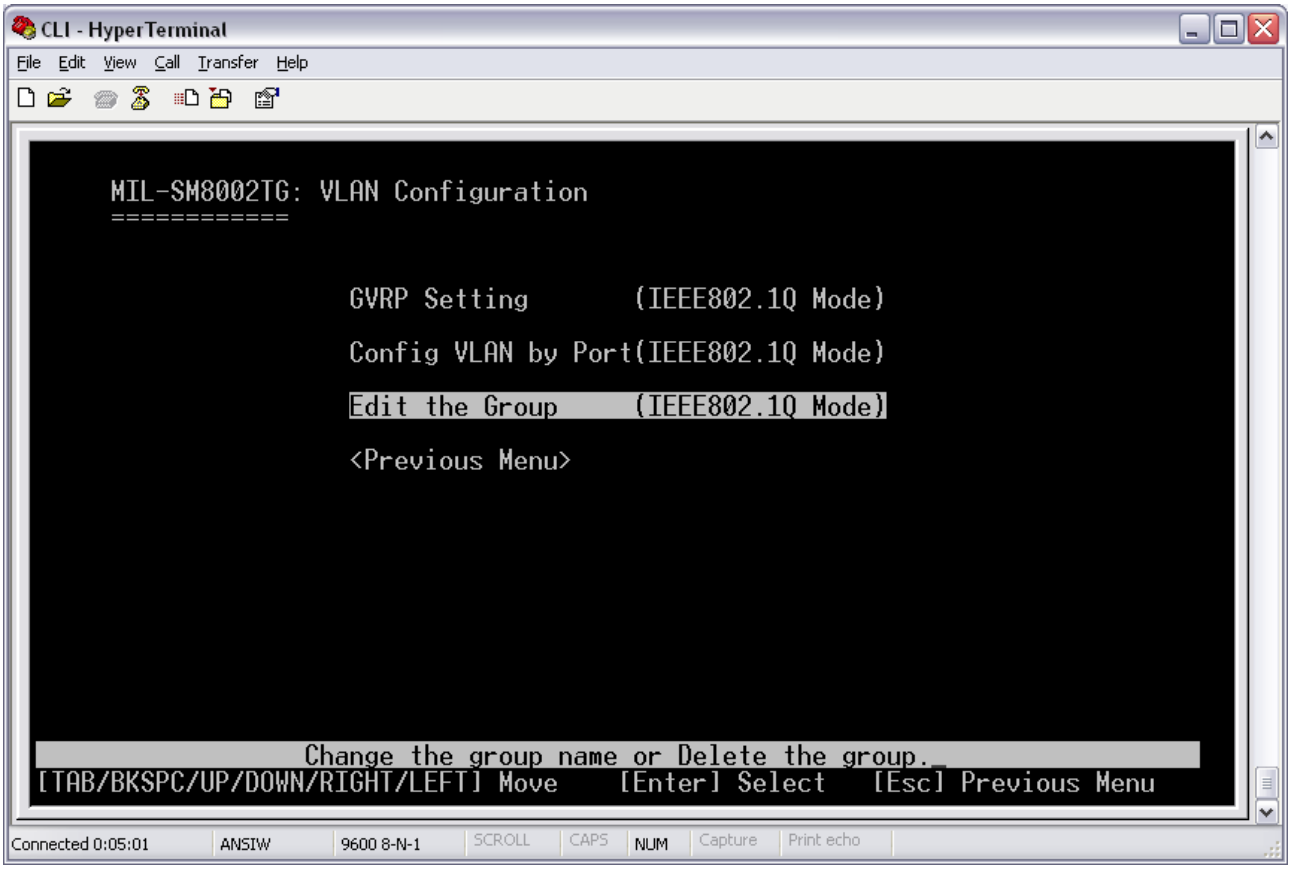
Display the all VLAN groups' information.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: VLAN List(IEEE802.1Q Mode)
-Group Name--------VID-------*****-----
Default 1 On
Edit all of VLAN group.
Connected 0:02:59 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Group List interface

802.1Q VLAN Configure

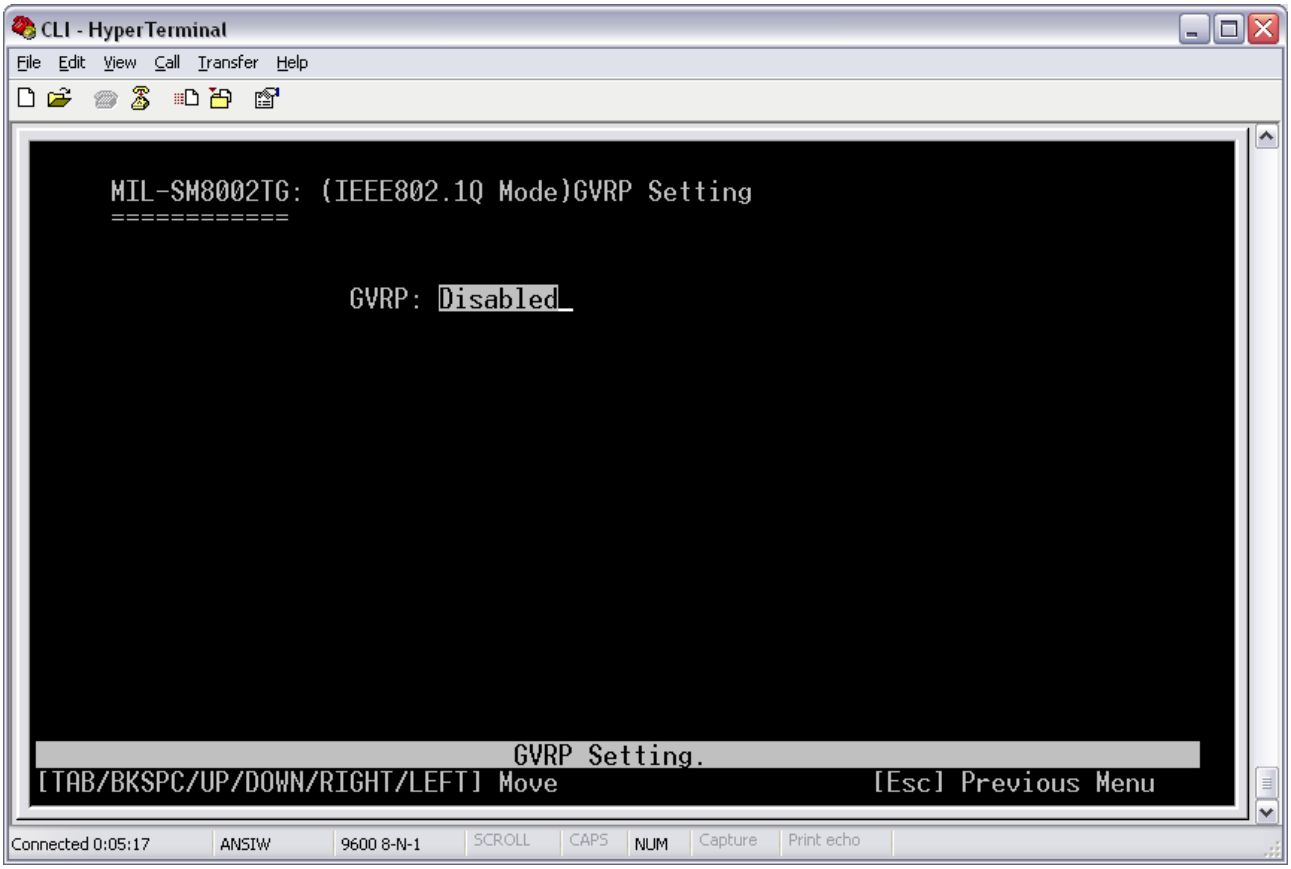
You configure GVRP setting, VLAN by port, and edit VLAN group.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: VLAN Configuration
GVRP Setting (IEEE802.1Q Mode)
Config VLAN by Port(IEEE802.1Q Mode)
Edit the Group (IEEE802.1Q Mode)
<Previous Menu>
Change the group name or Delete the group.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:05:01 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

802.1Q VLAN Configuration interface

GVRP Setting

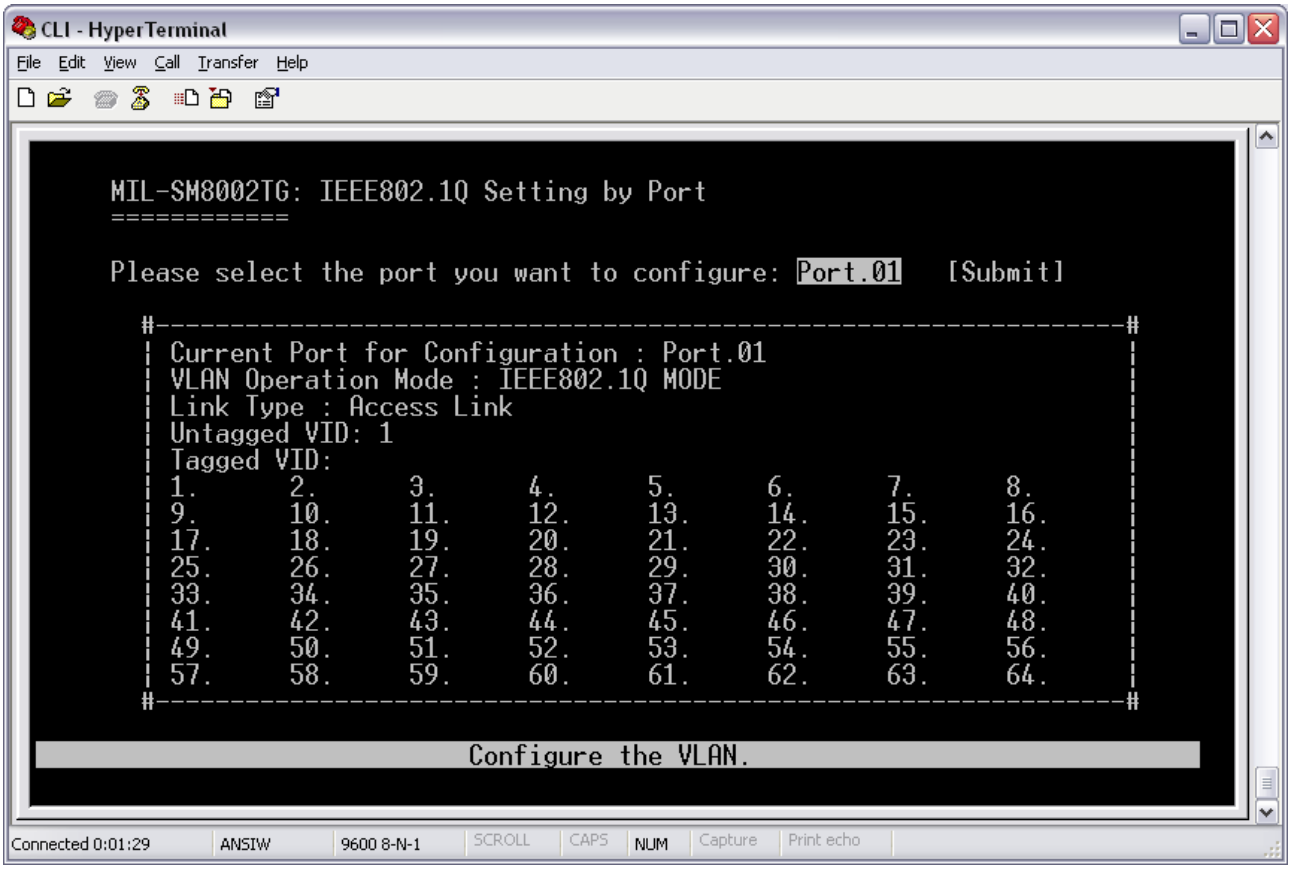
GVRP (Generic Attribute Registration Protocol) is an application defined in the IEEE 802.1Q standard that allows for the control of VLANs. Use **Space** key to change the GVRP setting – Disable or Enable. And then, select the **Save** to apply the setting.



GVRP Setting interface

Configure VLAN by Port

1. Select the port that wants to configure by using **Spec** key. **Submit** to get the port current setting.
2. **Link Type**: there are 3 link types.
3. **Untagged VID:** assign the untagged frame VID.
4. **Tagged VID:** assign the tagged frame VID.
5. **Save** the configuration.

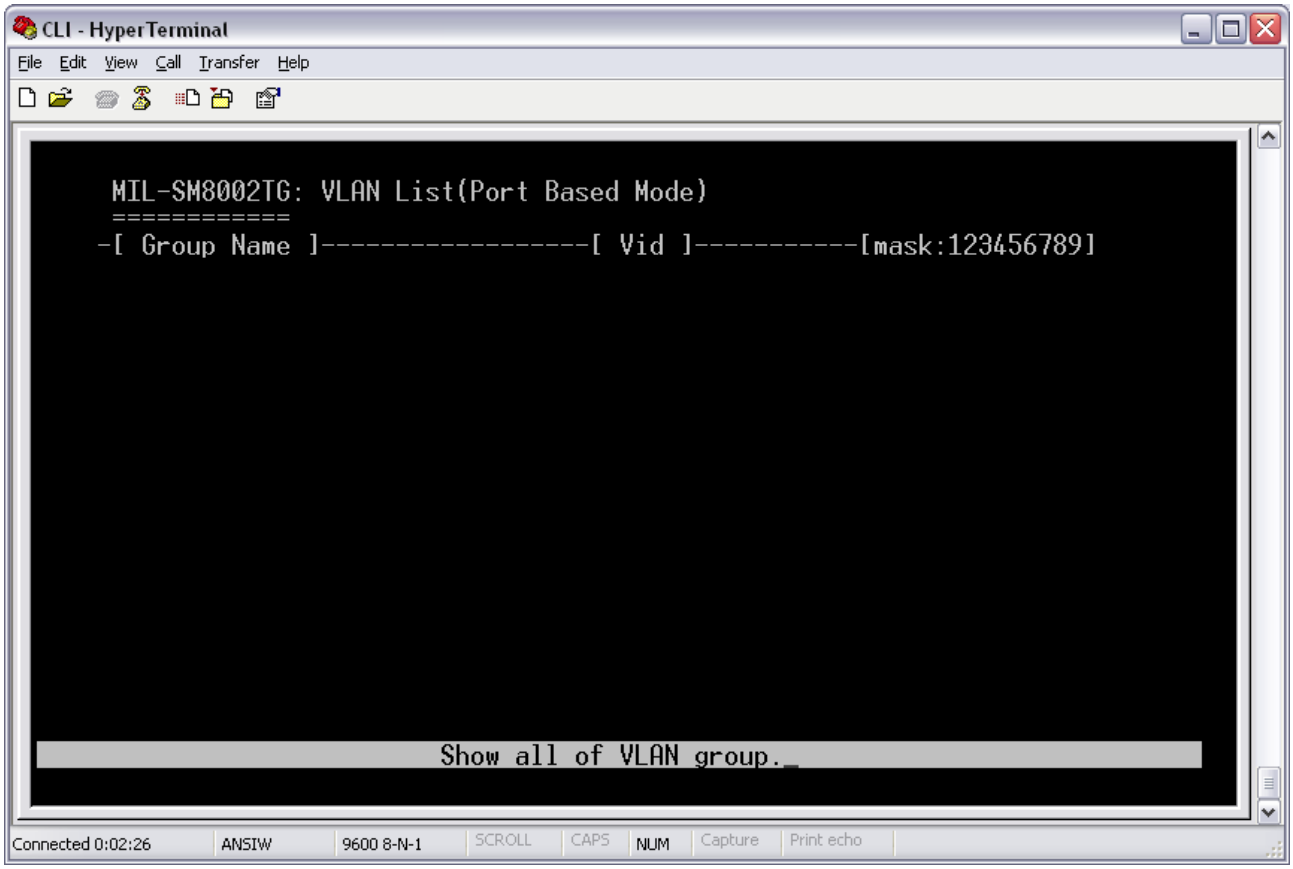

CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: IEEE802.1Q Setting by Port
Please select the port you want to configure: Port.01 [Submit]
Current Port for Configuration : Port.01
VLAN Operation Mode : IEEE802.1Q MODE
Link Type : Access Link
Untagged VID: 1
Tagged VID:
1. 2. 3. 4. 5. 6. 7. 8.
9. 10. 11. 12. 13. 14. 15. 16.
17. 18. 19. 20. 21. 22. 23. 24.
25. 26. 27. 28. 29. 30. 31. 32.
33. 34. 35. 36. 37. 38. 39. 40.
41. 42. 43. 44. 45. 46. 47. 48.
49. 50. 51. 52. 53. 54. 55. 56.
57. 58. 59. 60. 61. 62. 63. 64.
Configure the VLAN.
Connected 0:01:29 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Configure VLAN by Port interface

VLAN List

Enable or disable the VLAN group.

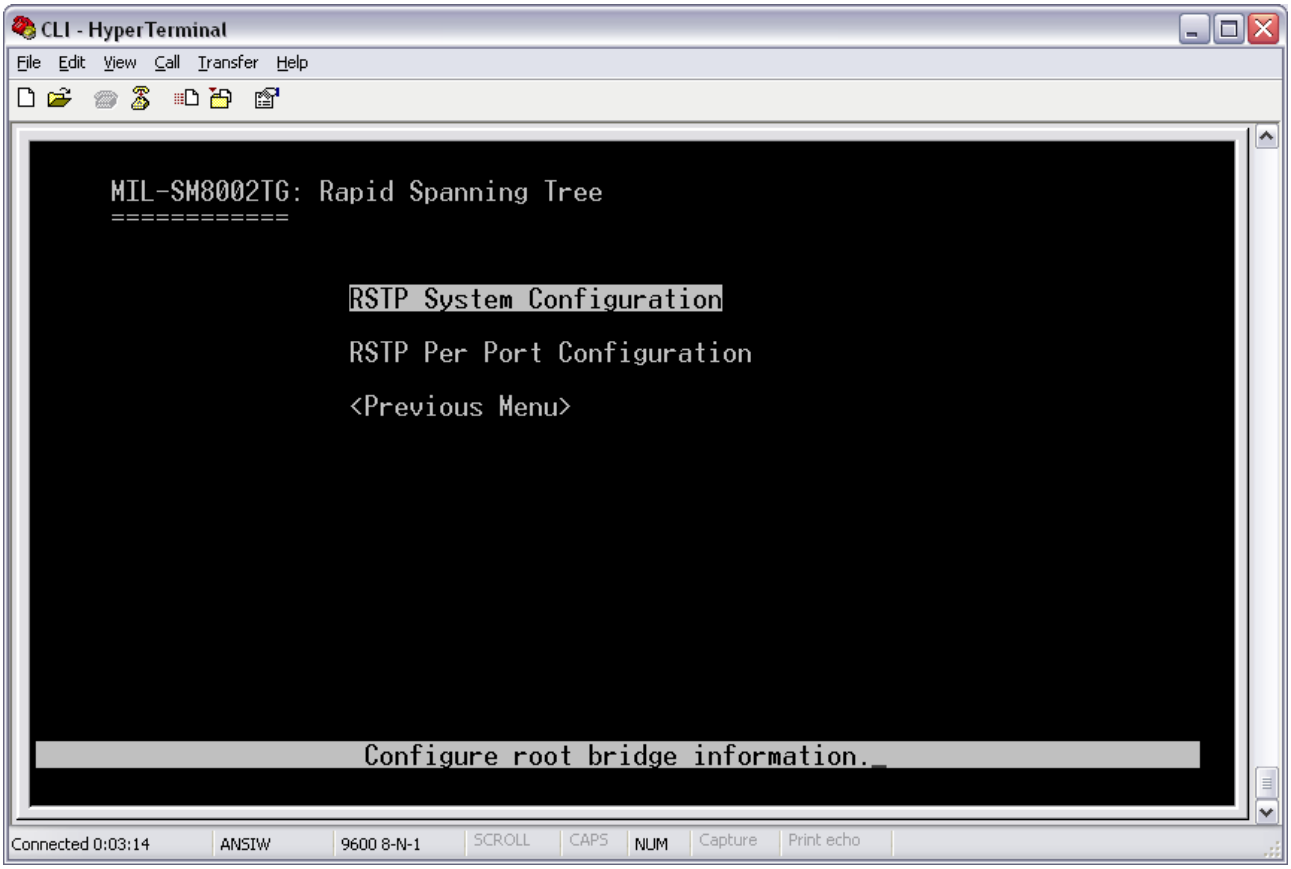
1. **Group Name:** you can rename the group name.
2. **On/Del:** On is active the VLAN group. Del is removing the VLAN group.
3. After editing, **Apply** the change.



Edit VLAN Group interface

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.



Rapid Spanning Tree interface

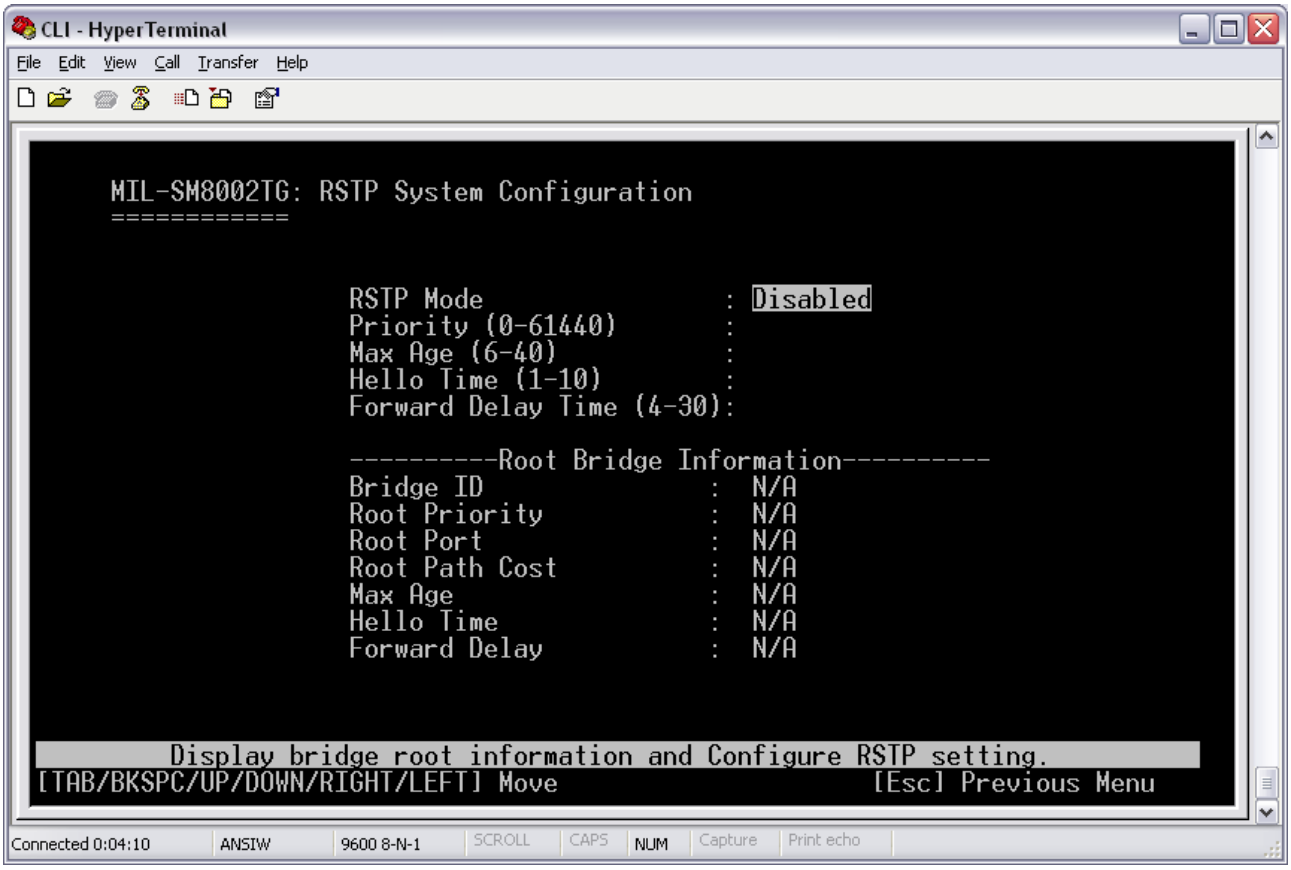
RSTP System Configuration

1. You can view spanning tree information about the Root Bridge.
2. You can modify RSTP state. After modification, **save** the configuration.
   - **RSTP mode:** you must enable or disable RSTP function before configure the related parameters.
   - **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If you change the value, you must reboot the switch assign path priority number. The value must be multiple of 4096 according to the protocol standard rule.
   - **Max Age (6-40):** the number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.

- **Hello Time (1-10):** the time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
- **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

[NOTE] Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.

2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

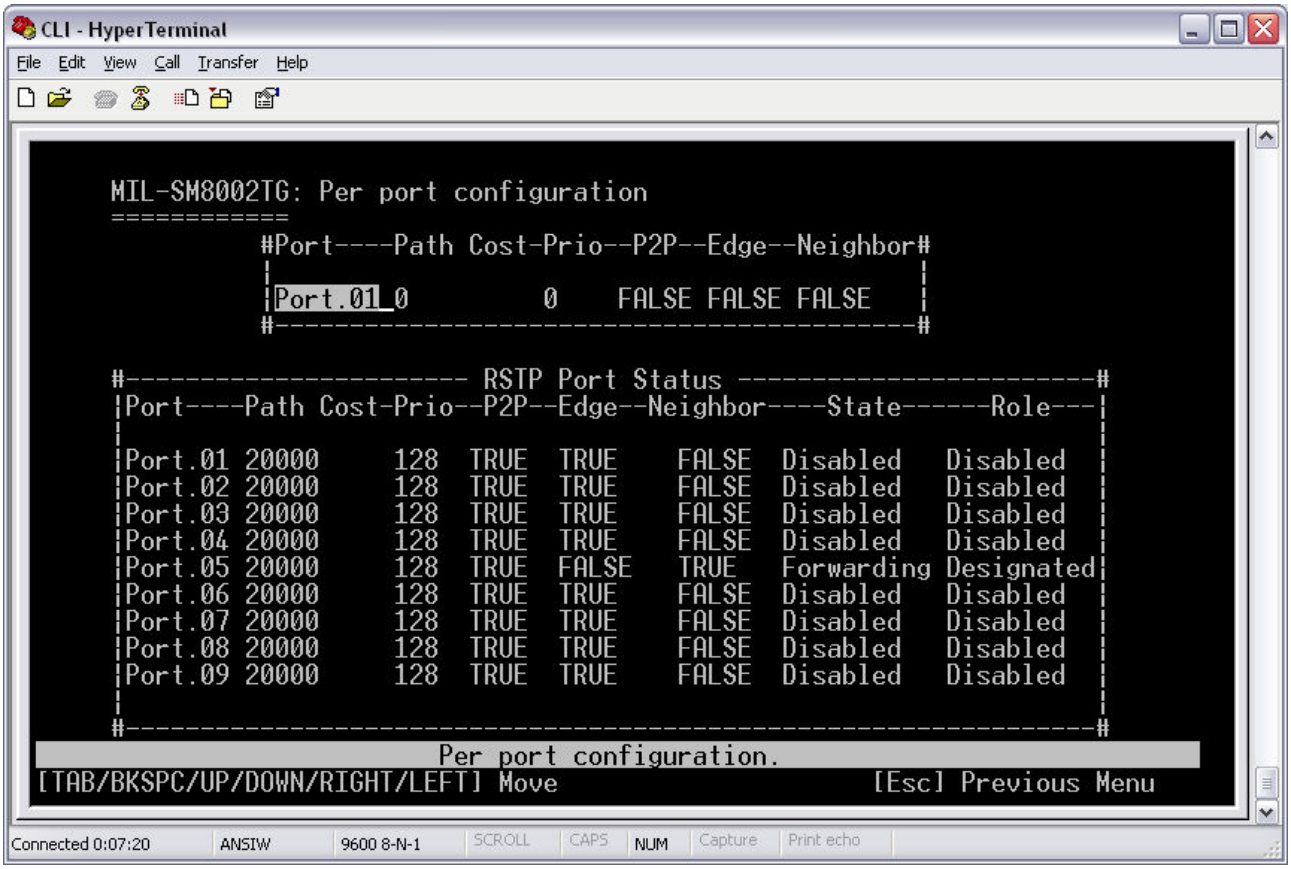

CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: RSTP System Configuration
RSTP Mode : Disabled
Priority (0-61440) :
Max Age (6-40) :
Hello Time (1-10) :
Forward Delay Time (4-30):
----------Root Bridge Information----------
Bridge ID : N/A
Root Priority : N/A
Root Port : N/A
Root Path Cost : N/A
Max Age : N/A
Hello Time : N/A
Forward Delay : N/A
Display bridge root information and Configure RSTP setting.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move
[Esc] Previous Menu
Connected 0:04:10 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

RSTP System Configuration interface

RSTP Per Port Configuration

You can configure path cost and priority of every port.

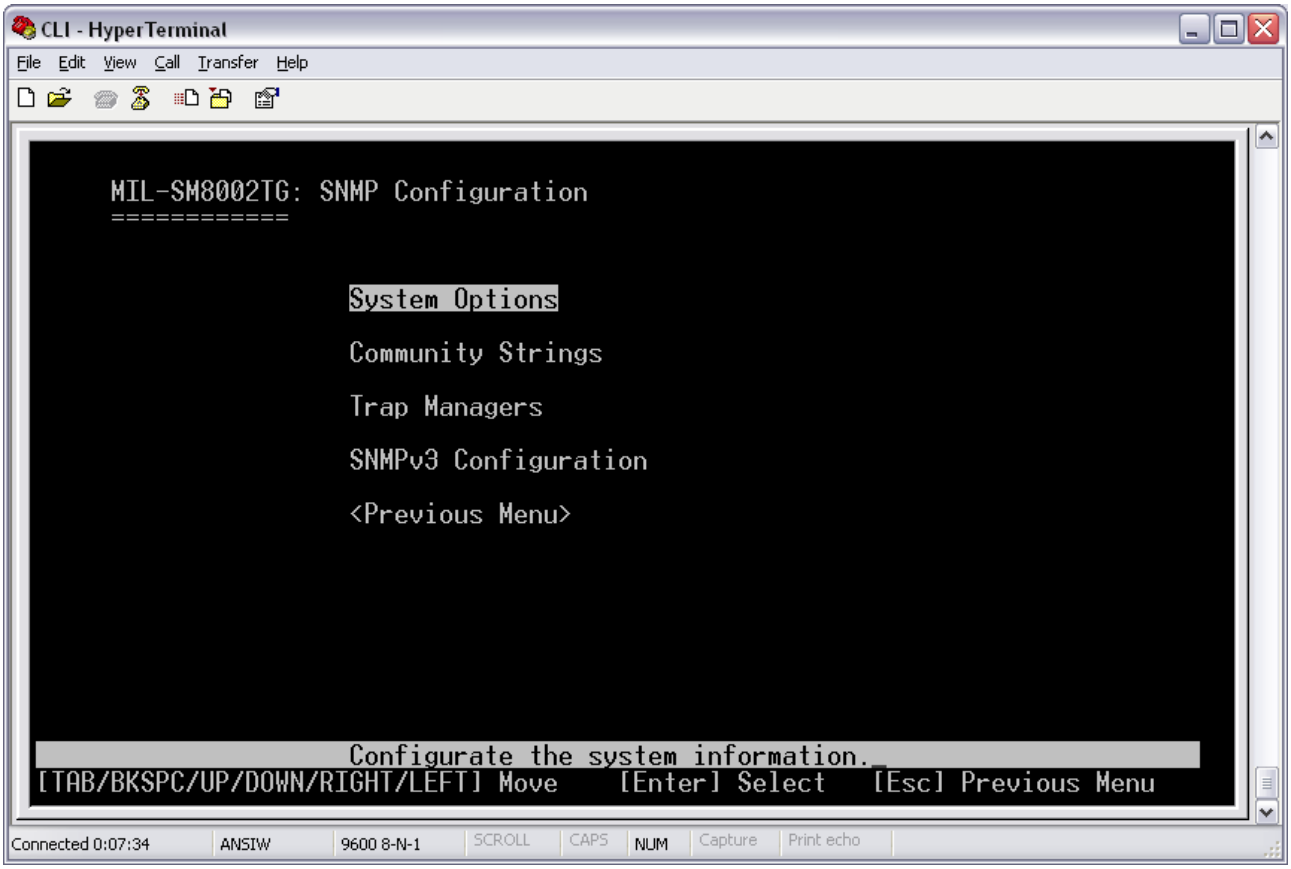
1. Select the port in Port column.
2. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
3. **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
4. **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
5. **Edge:** The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
6. **Neighbor:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
7. **Apply** the setting.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Per port configuration
#Port----Path Cost-Prio--P2P--Edge--Neighbor#
Port.01 0 0 FALSE FALSE FALSE
RSTP Port Status
Port----Path Cost-Prio--P2P--Edge--Neighbor----State------Role---
Port.01 20000 128 TRUE TRUE FALSE Disabled Disabled
Port.02 20000 128 TRUE TRUE FALSE Disabled Disabled
Port.03 20000 128 TRUE TRUE FALSE Disabled Disabled
Port.04 20000 128 TRUE TRUE FALSE Disabled Disabled
Port.05 20000 128 TRUE FALSE TRUE Forwarding Designated
Port.06 20000 128 TRUE TRUE FALSE Disabled Disabled
Port.07 20000 128 TRUE TRUE FALSE Disabled Disabled
Port.08 20000 128 TRUE TRUE FALSE Disabled Disabled
Port.09 20000 128 TRUE TRUE FALSE Disabled Disabled
Per port configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move
[Esc] Previous Menu
Connected 0:07:20
ANSIW
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

RSTP Per Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

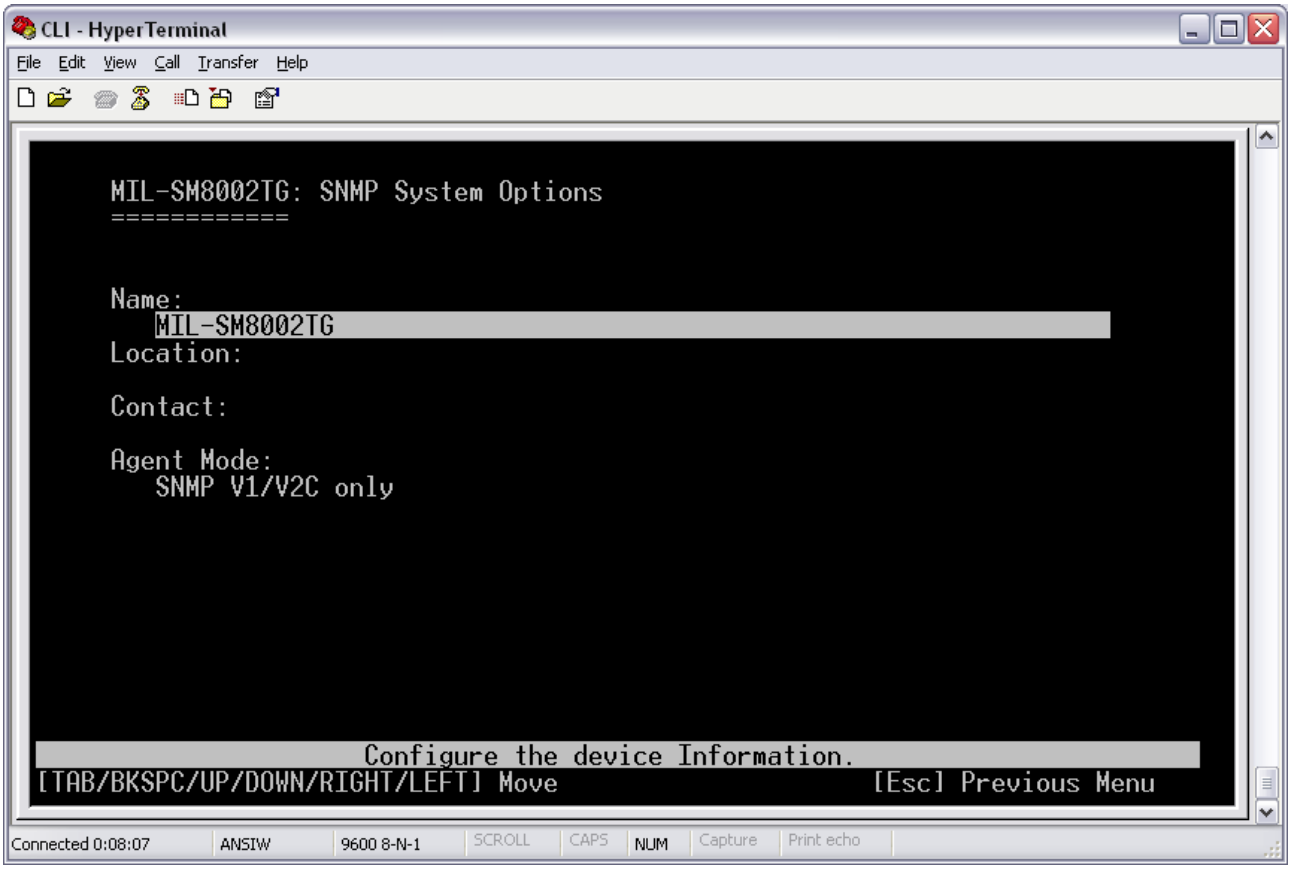

CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: SNMP Configuration
System Options
Community Strings
Trap Managers
SNMPv3 Configuration
<Previous Menu>
Configurate the system information.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:07:34 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

SNMP Configuration interface

System Options

Enter the system name, contact, and location information.

1. **Name:** assign a name for the switch.
2. **Contact:** Type the name of contact person or organization.
3. **Location:** Type the location of the switch.
4. **Agent Mode:** Select the SNMP version that you want to use it.
5. **<Save>** to save configure value.



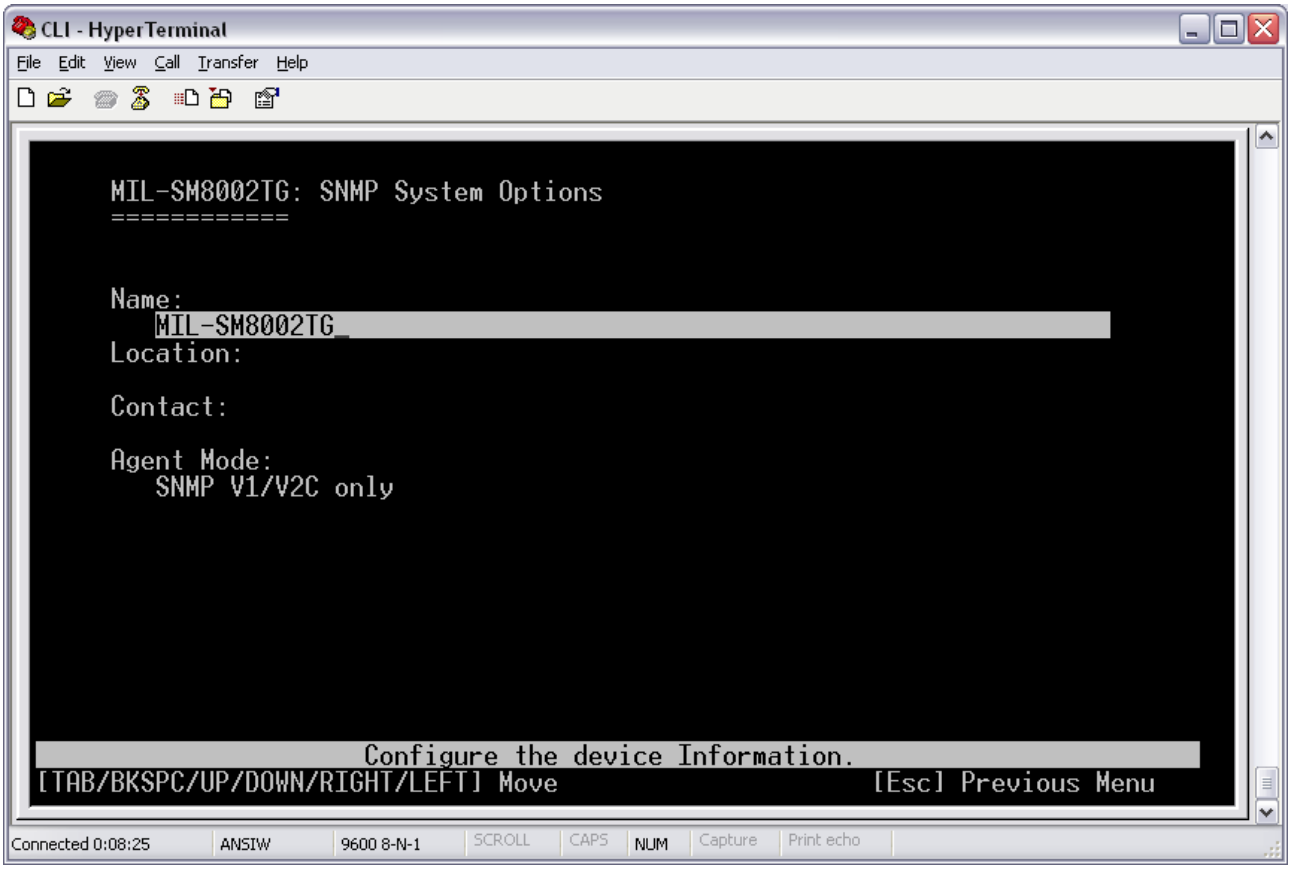
SNMP System Options interface

Community Strings

You can change the default community string that public and private attribute and define two more set community string.

1. **Community Name:** It uses for authenticating the manager to allow access the agent. Type the name of community strings. The Public and Private Community string cannot be changed the name.
2. **Attribute:** enable the access rights is read only or read/write or string removed.
   - **Read only:** Read only, enables requests accompanied by this string to display MIB-object information.
   - **Read/Write:** Read write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.
   - **String Removed:** this community string is disabling.

3. **Save** the configuration.



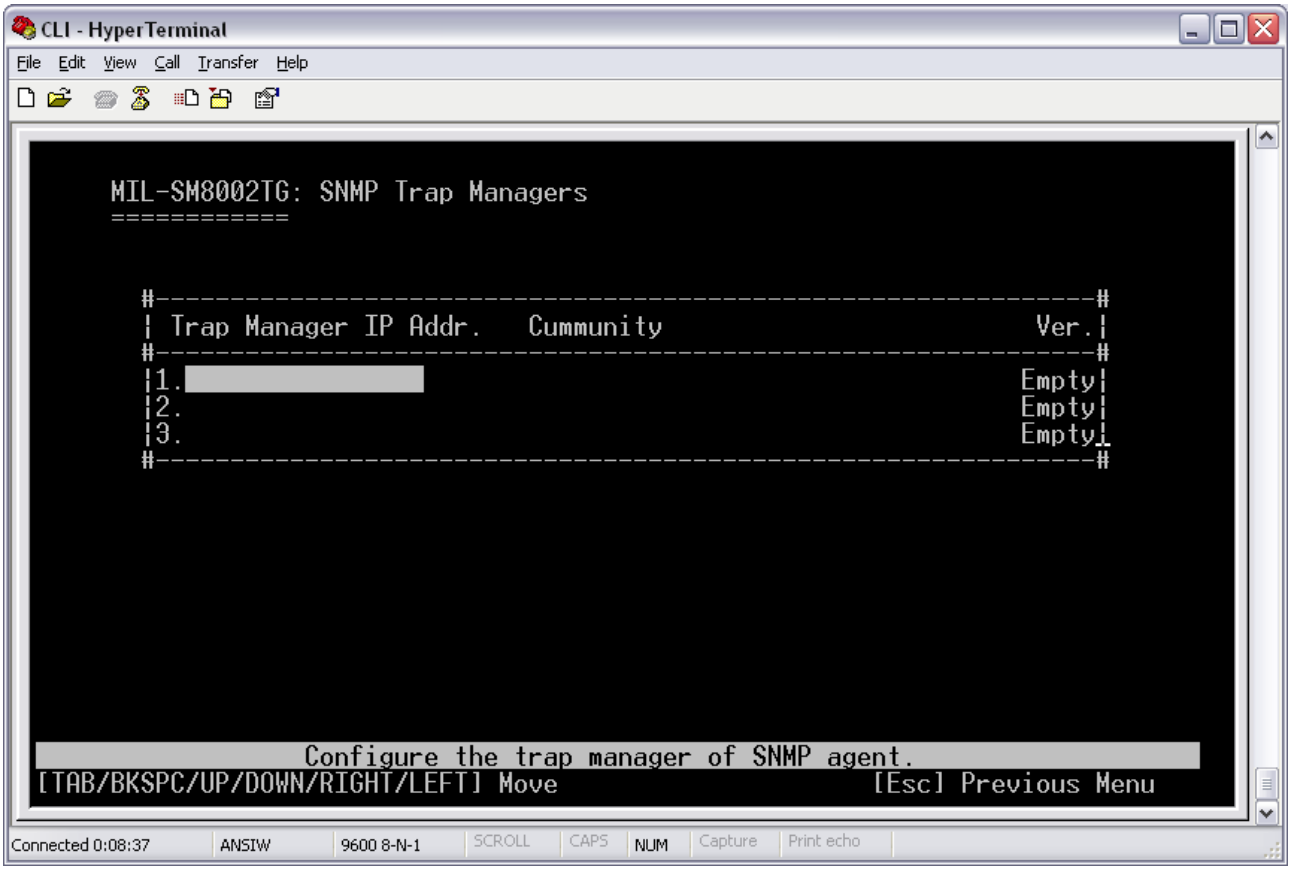
Add Community Strings interface

Trap Managers

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

1. **Trap Manager IP:** enter the IP address of trap manager.
2. **Community Name:** enter the community string.
3. **Ver.:** select the SNMP version type – v 1 or v2.
4. **<Save>** to save all configure

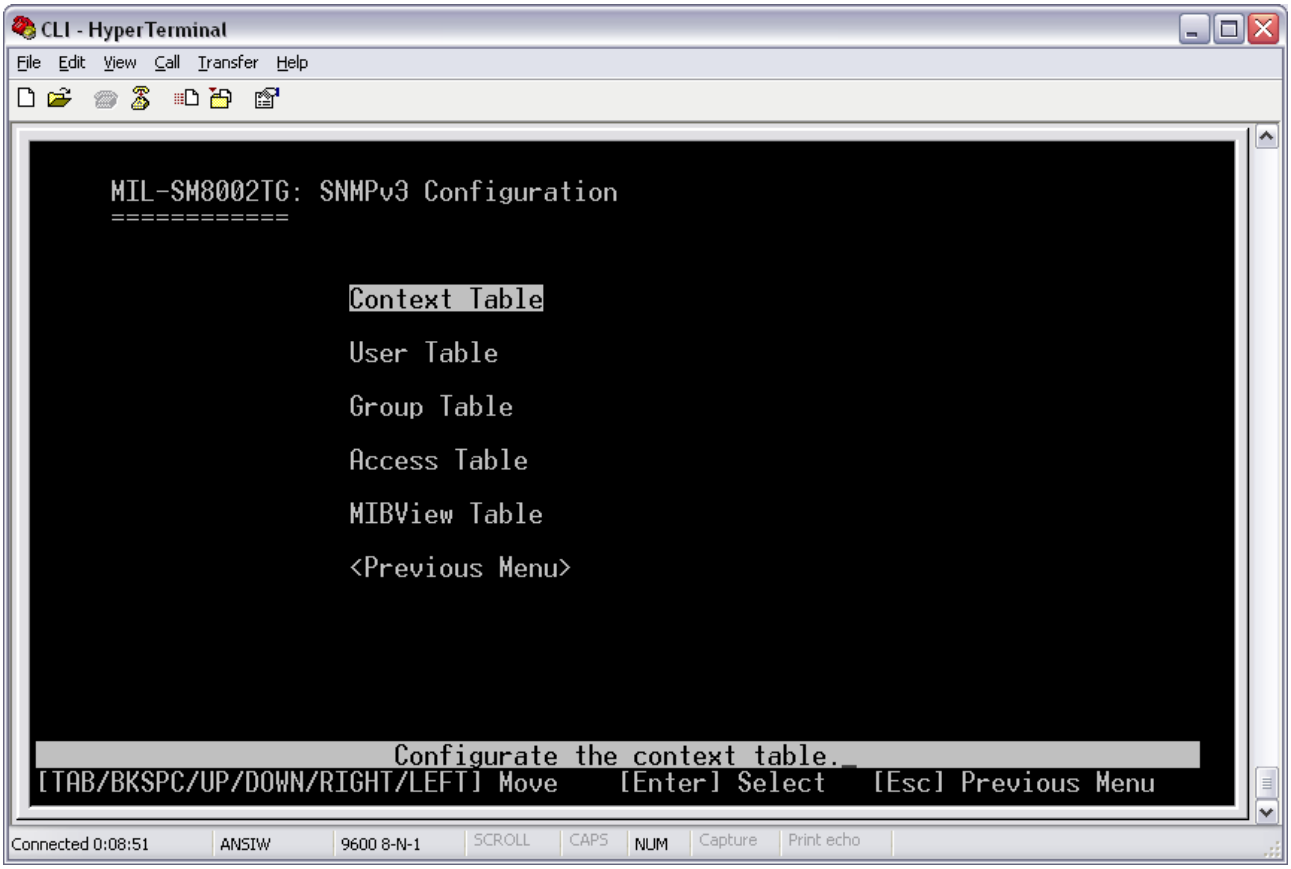
5. To disable the trap manager, please delete the trap manager IP, community string and version. And then, save to change.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: SNMP Trap Managers
Trap Manager IP Addr. Cummunity Ver.
1. Empty
2. Empty
3. Empty
Configure the trap manager of SNMP agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Esc] Previous Menu
Connected 0:08:37 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Trap Managers interface

SNMP V 3 Configuration

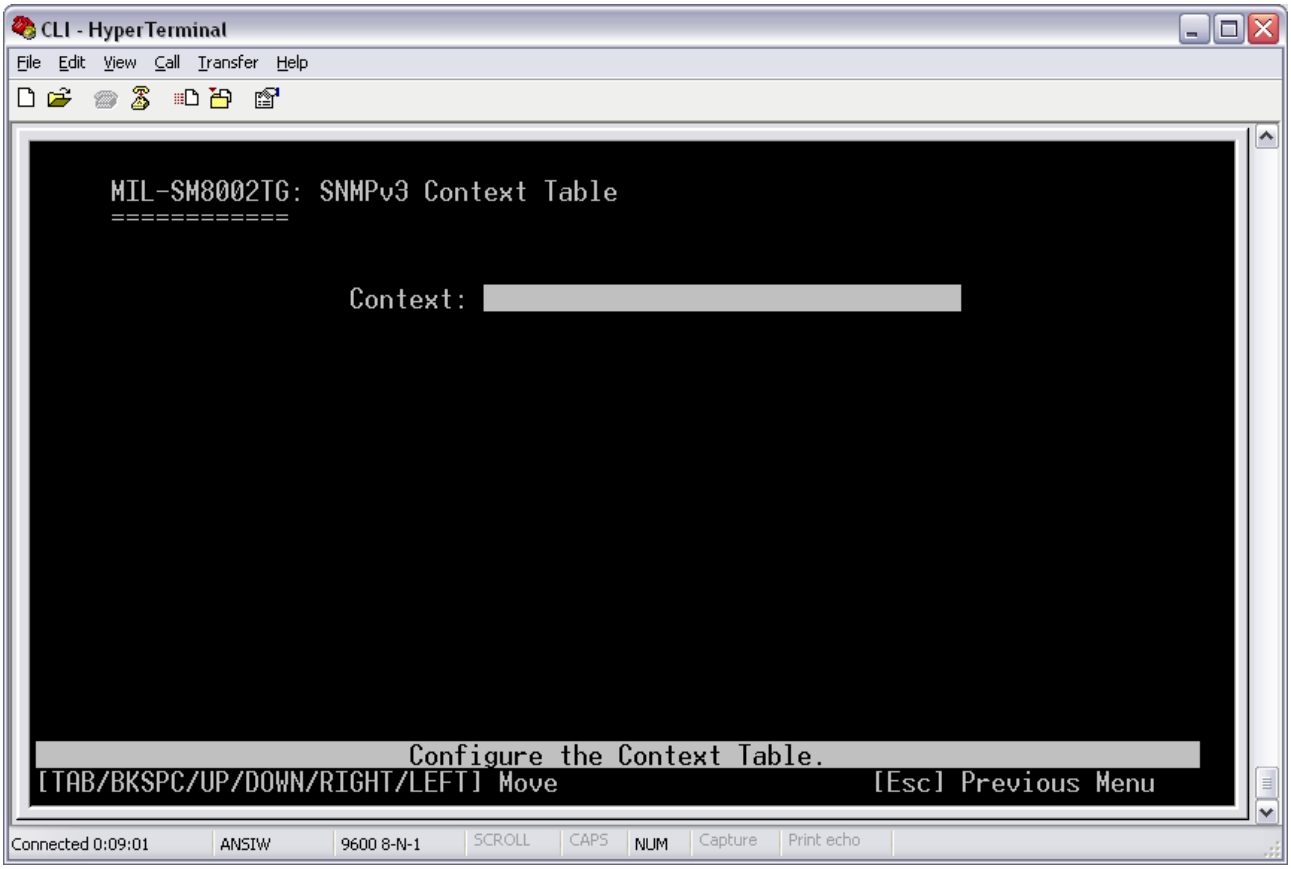
Configure the SNMP V3 function.



SNMP V3 configuration interface

Context Table

Configure SNMP v3 context table. Assign the context name of context table.

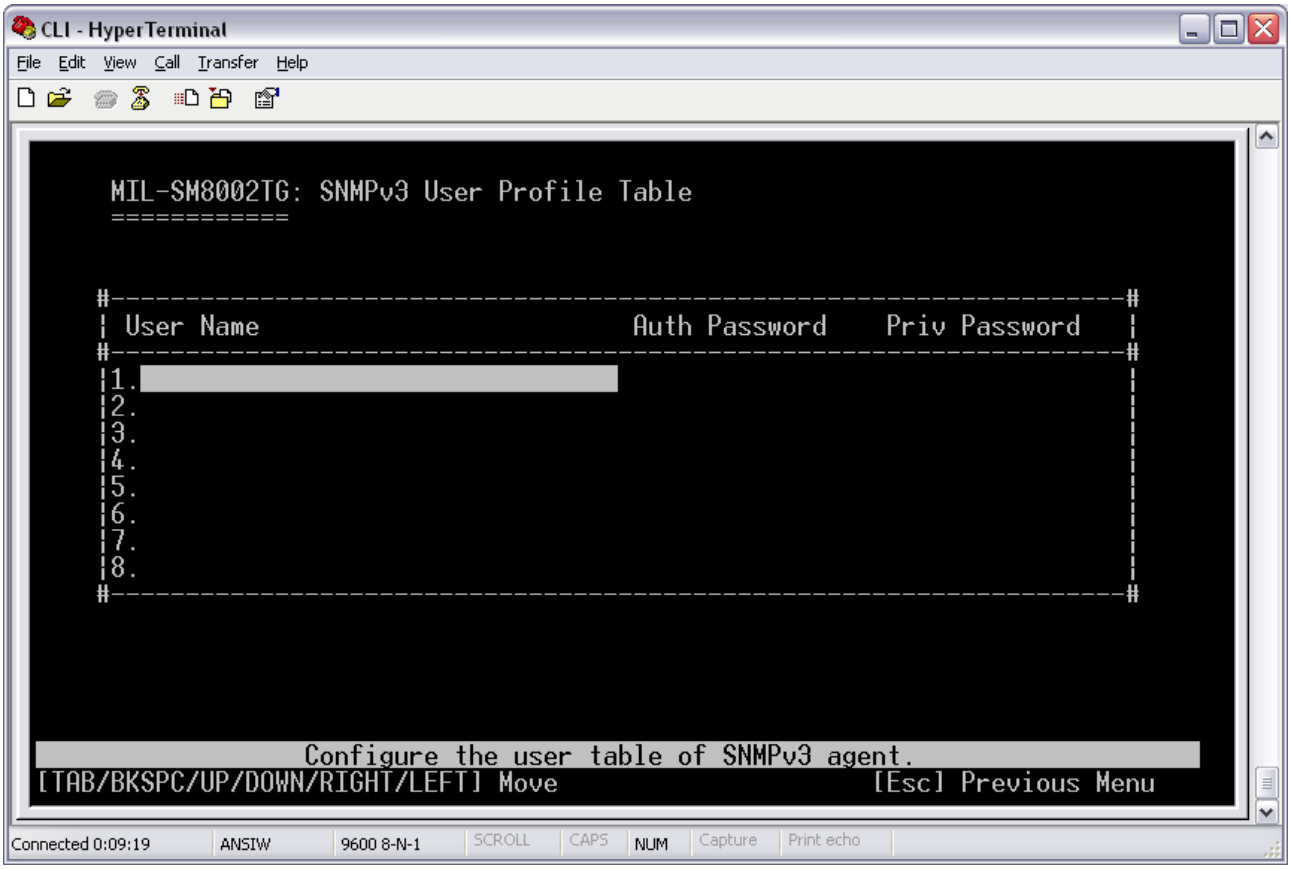


SNMP v3_Context Table interface

User Table

Configure SNMP v3 user table..

1. **User Name:** set up the user name.
2. **Auth Password:** set up the authentication password.
3. **Priv Password:** set up the private password.
4. **<Save>** to save all configure

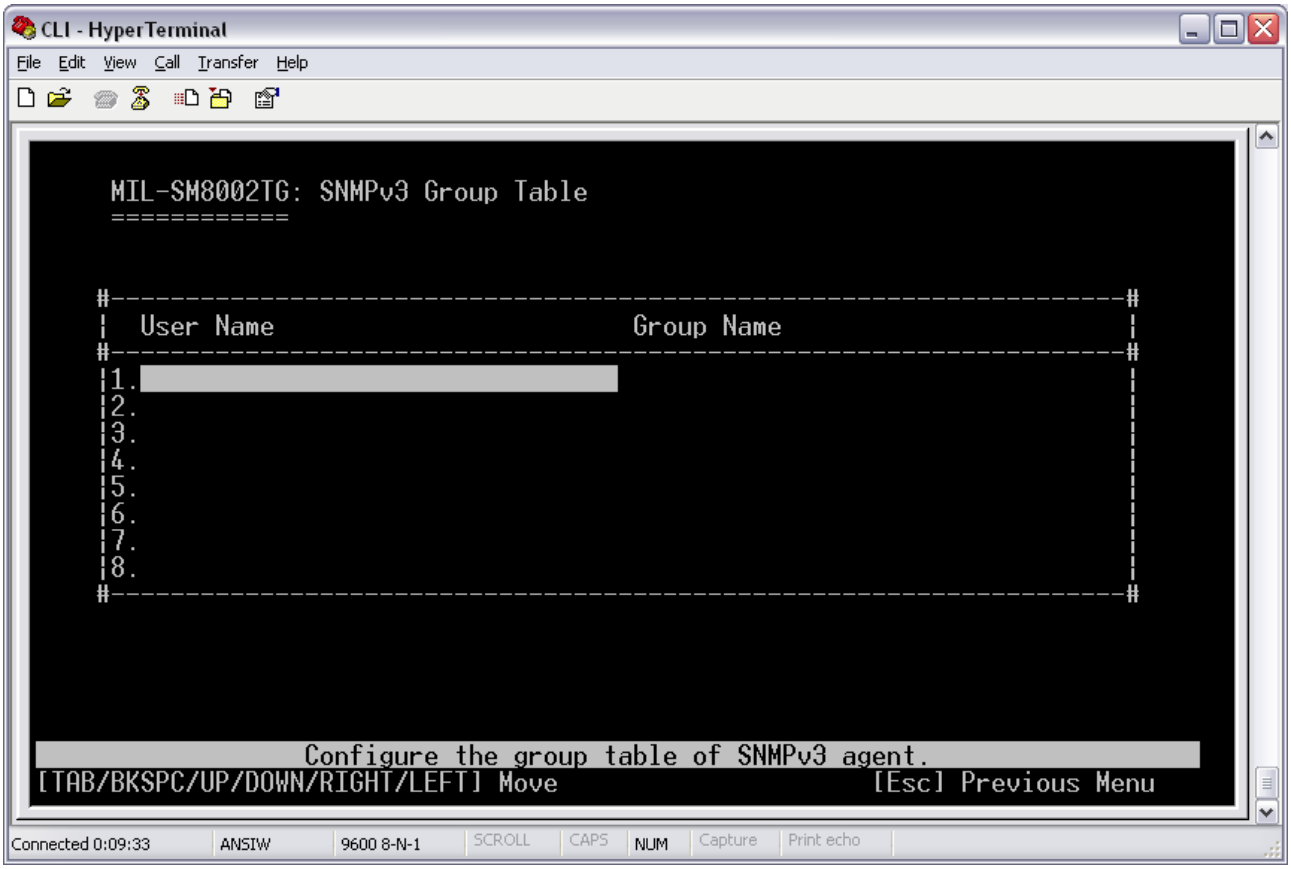


SNMP v3_User Table interface

Group Table

Configure SNMP v3 group table.

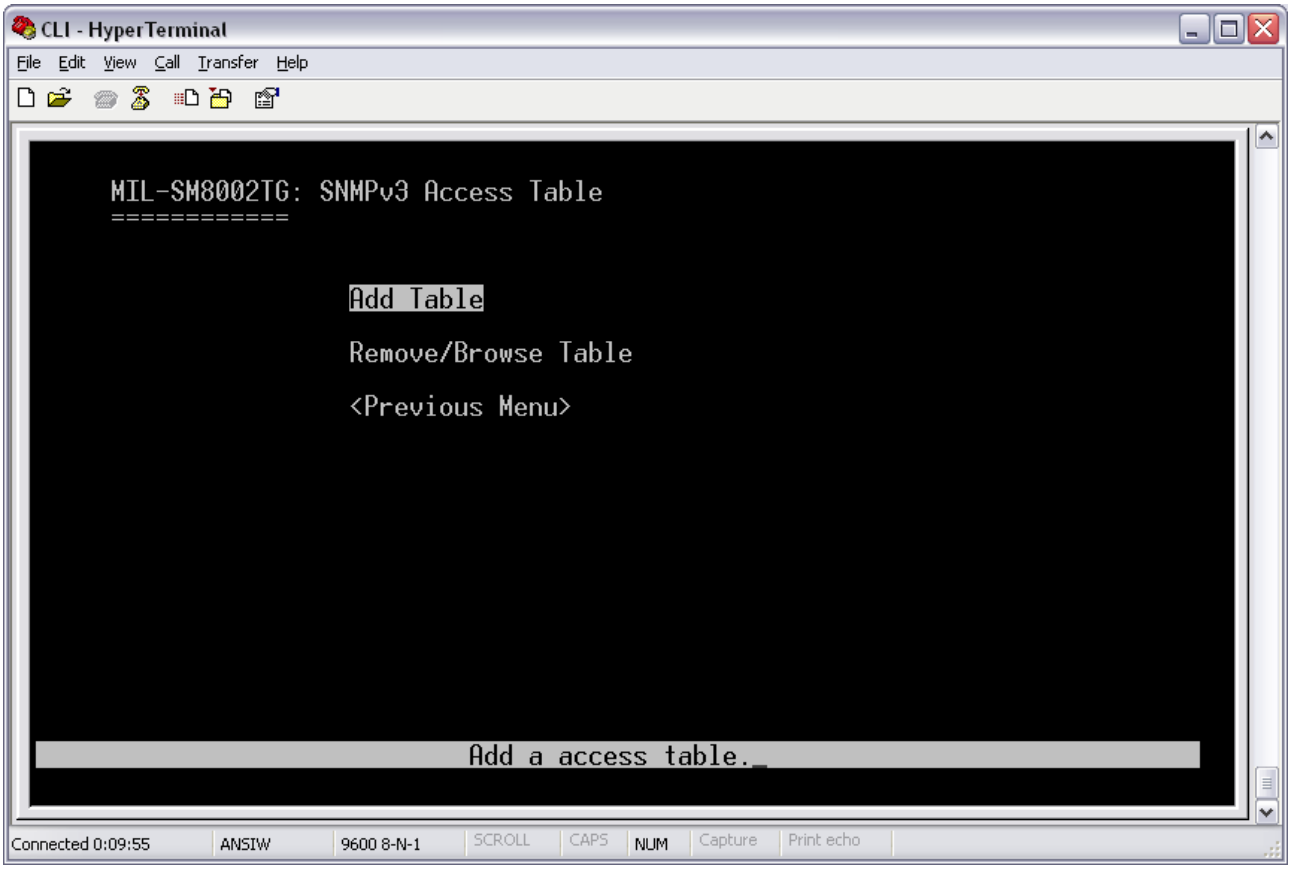
1. **User Name:** assign the user name that you have set up in user table.
2. **Group Name:** set up the group name.
3. **<Save>** to save all configure



SNMP v3_Group Table interface

Access Table

Configure SNMP v3 access table.

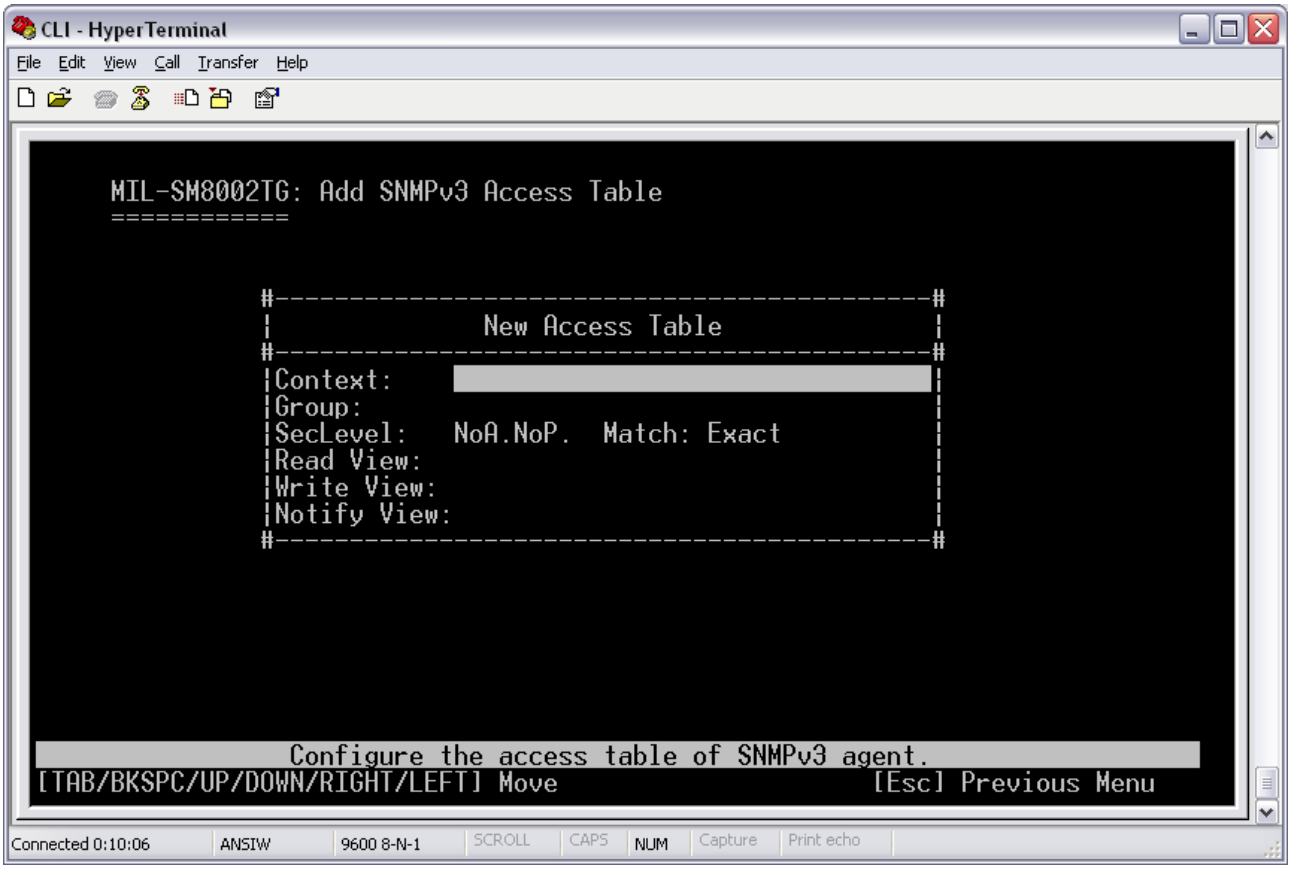


SNMP v3_AccessTable interface

- **Add Table**

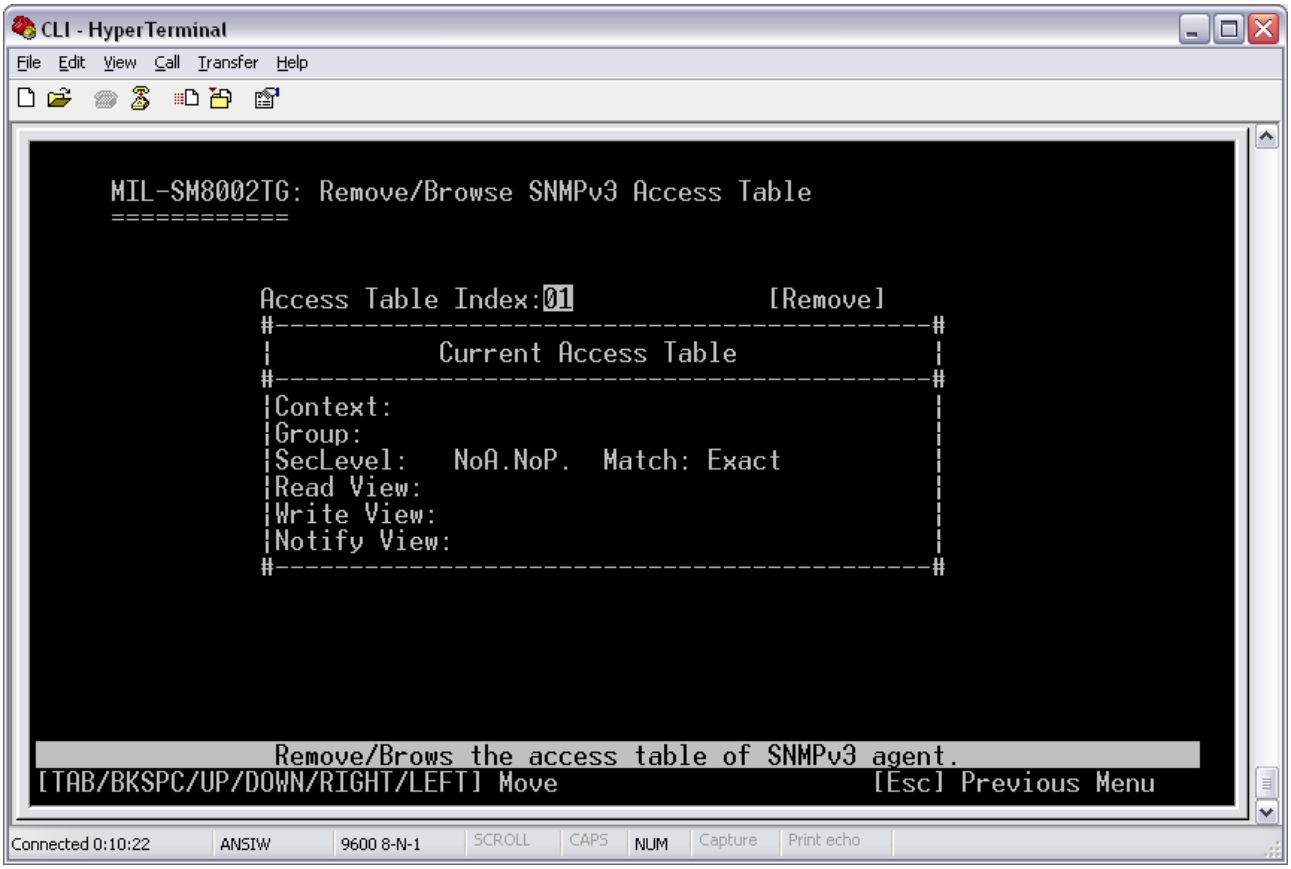
Add the access table.

1. **Context:** set up the context name.
2. **Group:** set up the group.
3. **Sec Level:** select the access level.
4. **Read View:** set up the read view.
5. **Write View:** set up the write view.
6. **<Save>** to save all configure



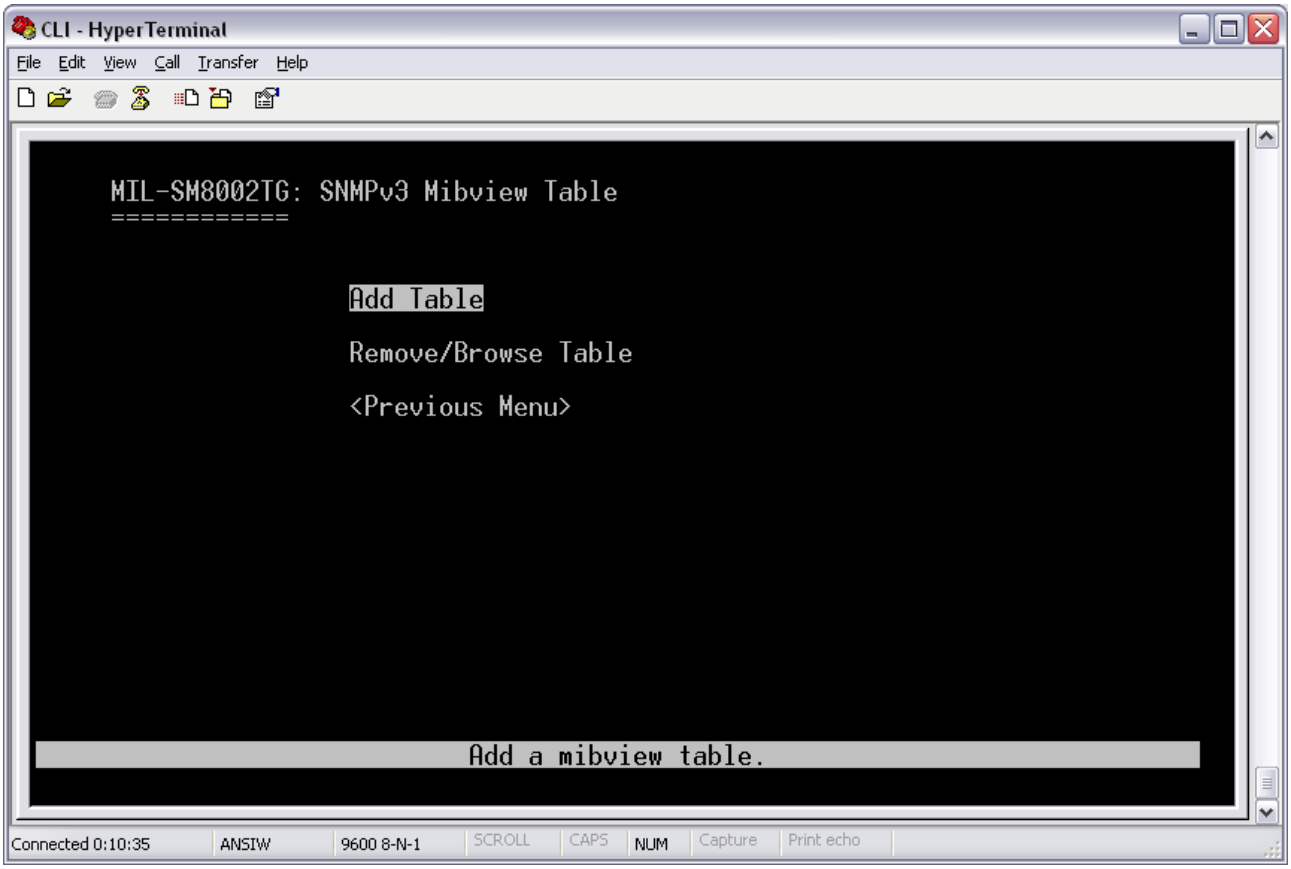
■ Remove/Browse Table

Remove and Browse access table.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Remove/Browse SNMPv3 Access Table
Access Table Index:01 [Remove]
Current Access Table
Context:
Group:
SecLevel: NoA.NoP. Match: Exact
Read View:
Write View:
Notify View:
Remove/Brows the access table of SNMPv3 agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Esc] Previous Menu
Connected 0:10:22 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

MIBview Table

Configure MIB view table.

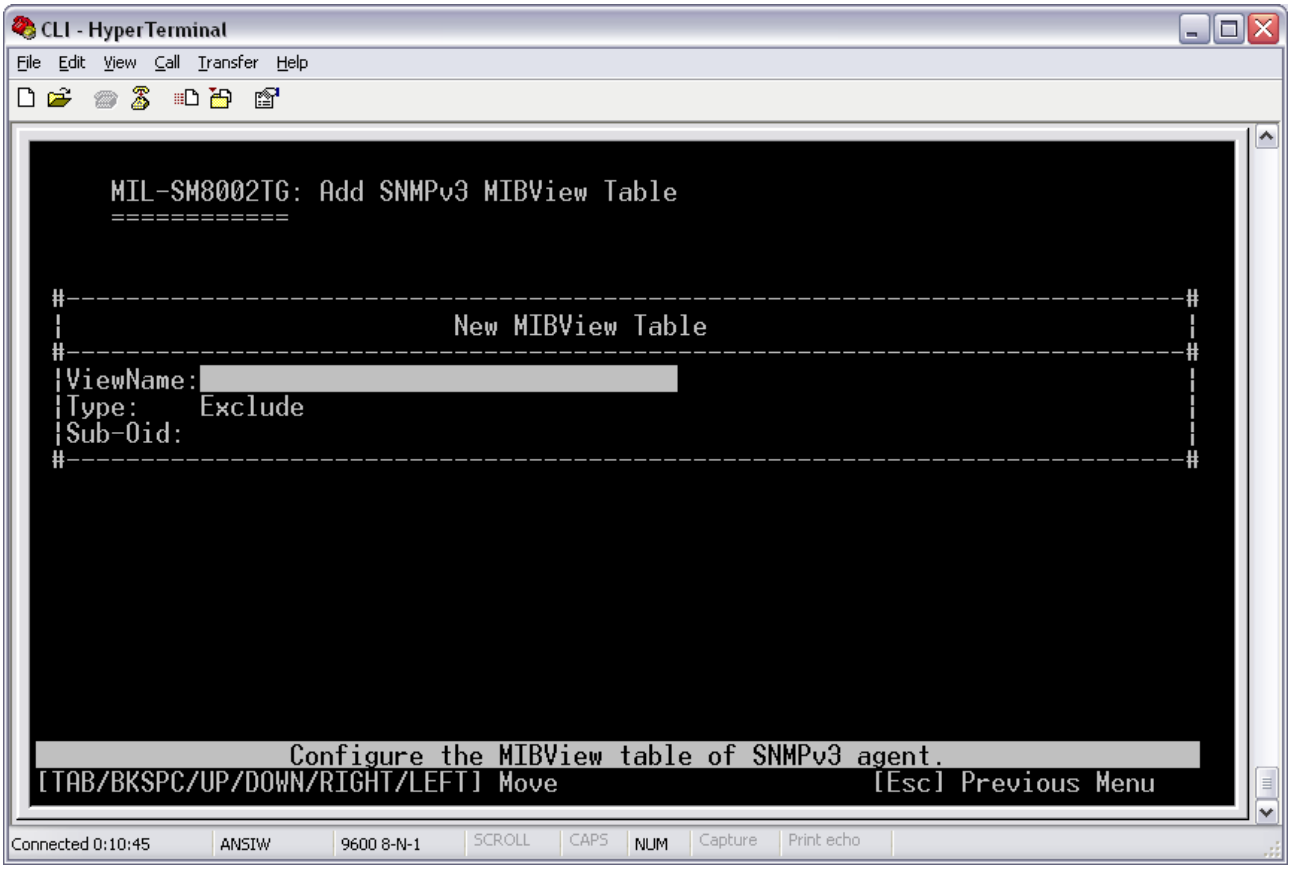


SNMP v3_MIBviewTable interface

■ Add Table

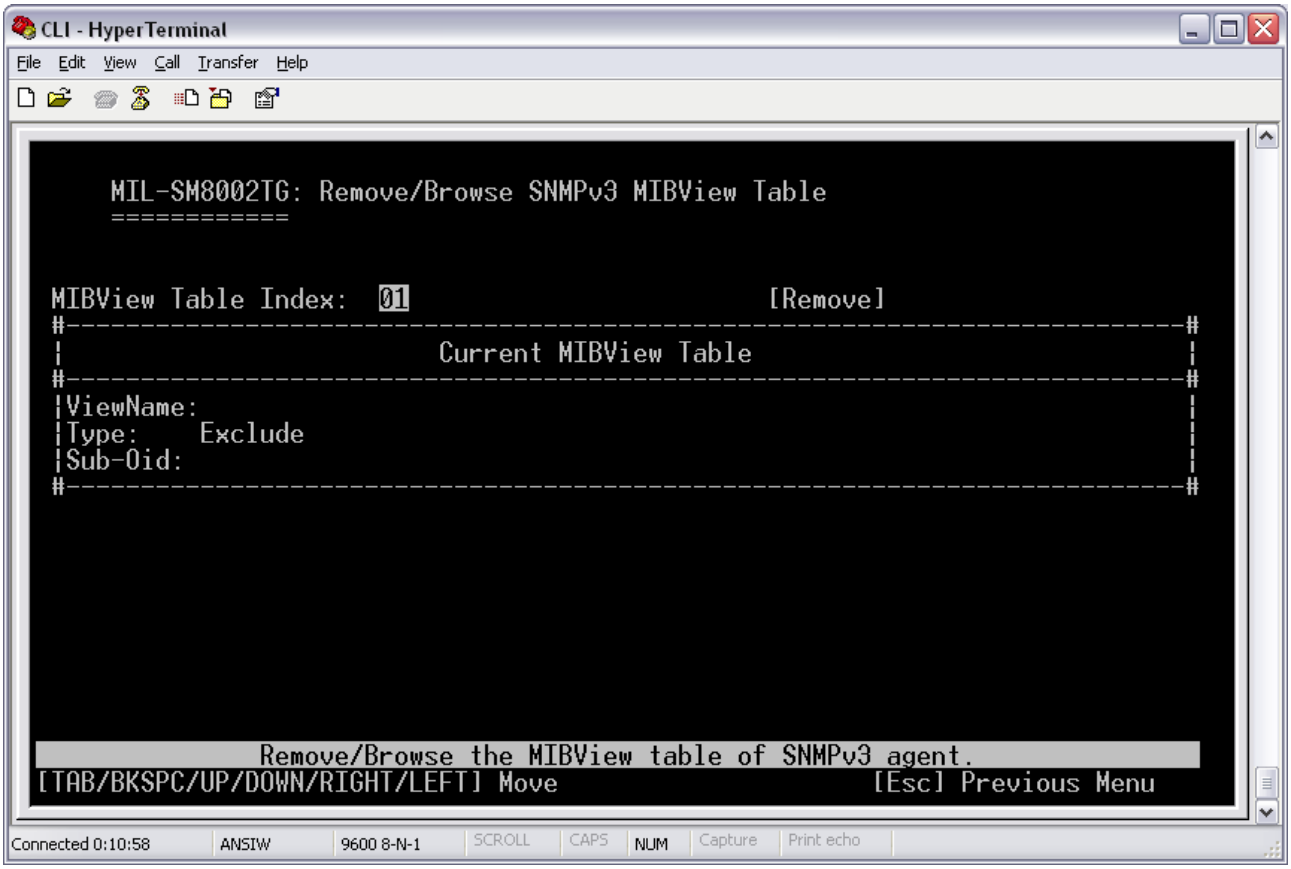
Add MIB view table.

1. **ViewName:** set up the name.
2. **Type:** select the type – exclude or include.
3. **Sub-Oid:** fill the Sub OID.
4. **<Save>** to save all configure



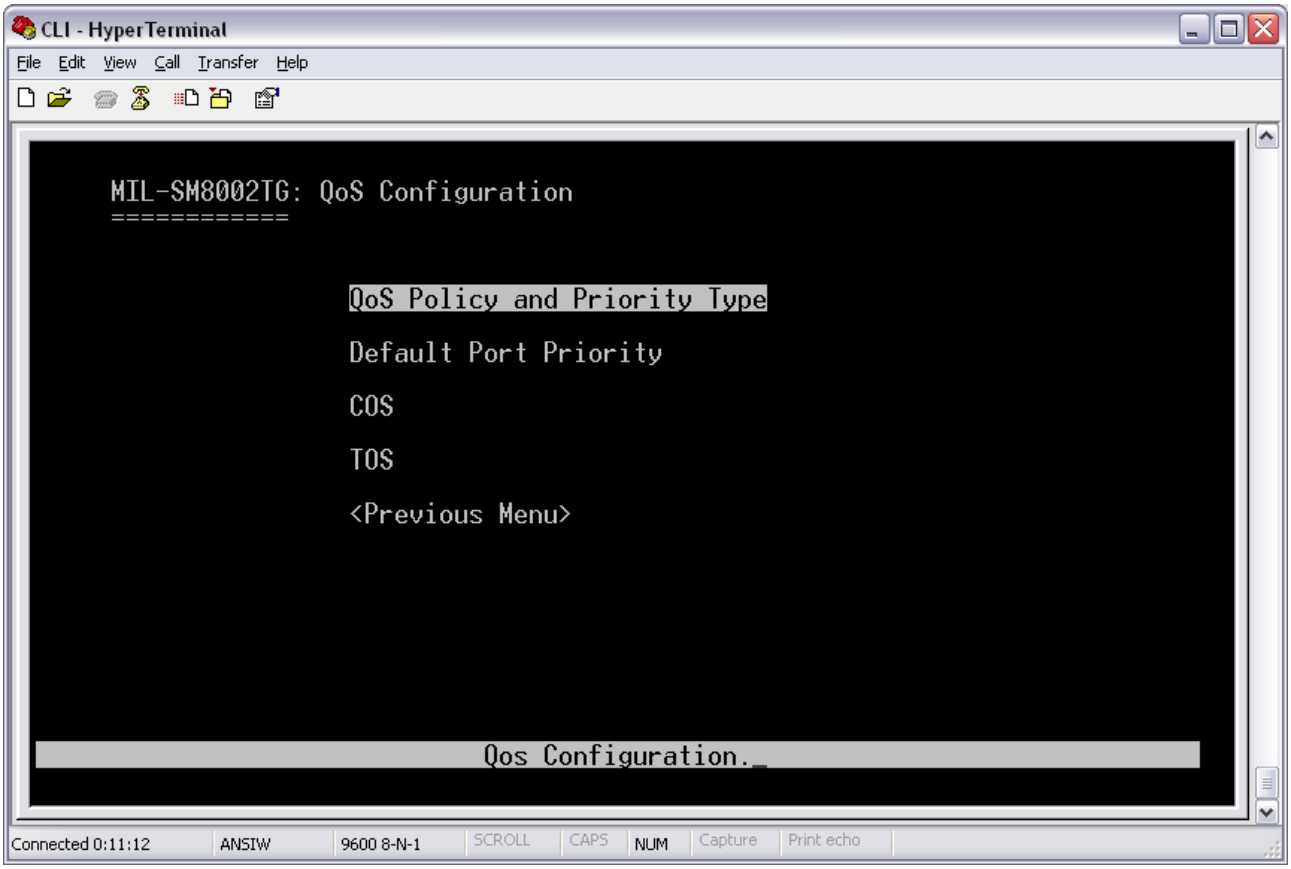
■ Remove/Browse Table

Remove and Browse MIBview table.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Remove/Browse SNMPv3 MIBView Table
MIBView Table Index: 01 [Remove]
Current MIBView Table
ViewName:
Type: Exclude
Sub-Oid:
Remove/Browse the MIBView table of SNMPv3 agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Esc] Previous Menu
Connected 0:10:58 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

QoS Configuration

You can configure Qos policy and priority setting, per port priority setting, COS and TOS setting.



QoS Configuration interface

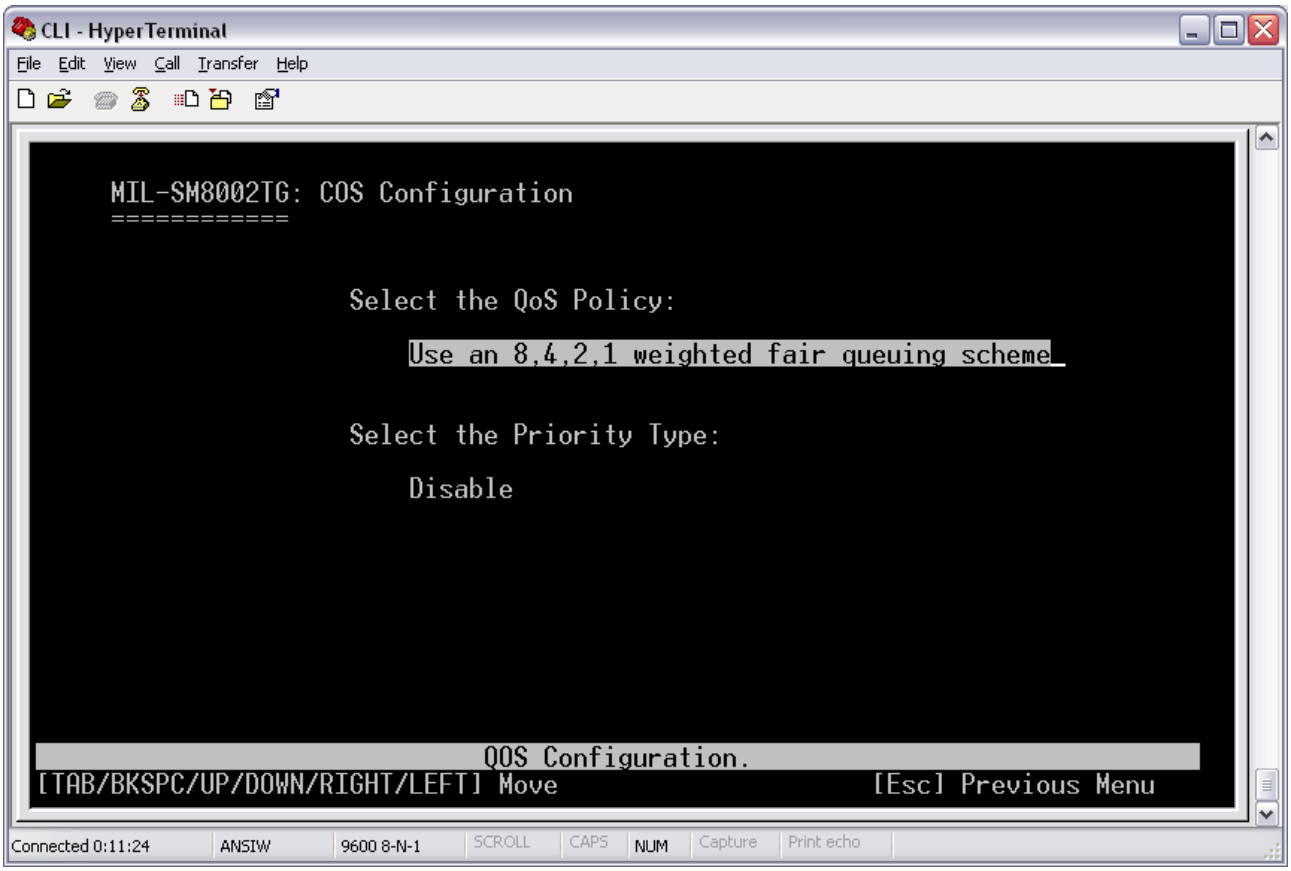
QoS Policy and Priority Type

- **Select the Oos Policy:** select the Qos policy rule.
  - **Using the 8,4,2,1 wnine fair queue scheme:** the switch will follow 8:4:2:1 rate to process priority queue from Hi to lowest queue. For example: the system will process 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets at the same time.
  - **Use the strict priority scheme:** Always higher queue will be process first, except higher queue is empty.
- **Select the Priority Type:** every port has 5 priority type selections. Disable means no priority type is selected.
  - **Port-base:** the port priority will follow the **default port priority** that you have assigned – High, middle, low, or lowest.
  - **COS only:** the port priority will only follow the **COS priority** that you have

assigned.

- **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
- **COS first:** the port priority will follow the COS priority first, and then other priority rule.
- **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.

■ **Save** the configuration.



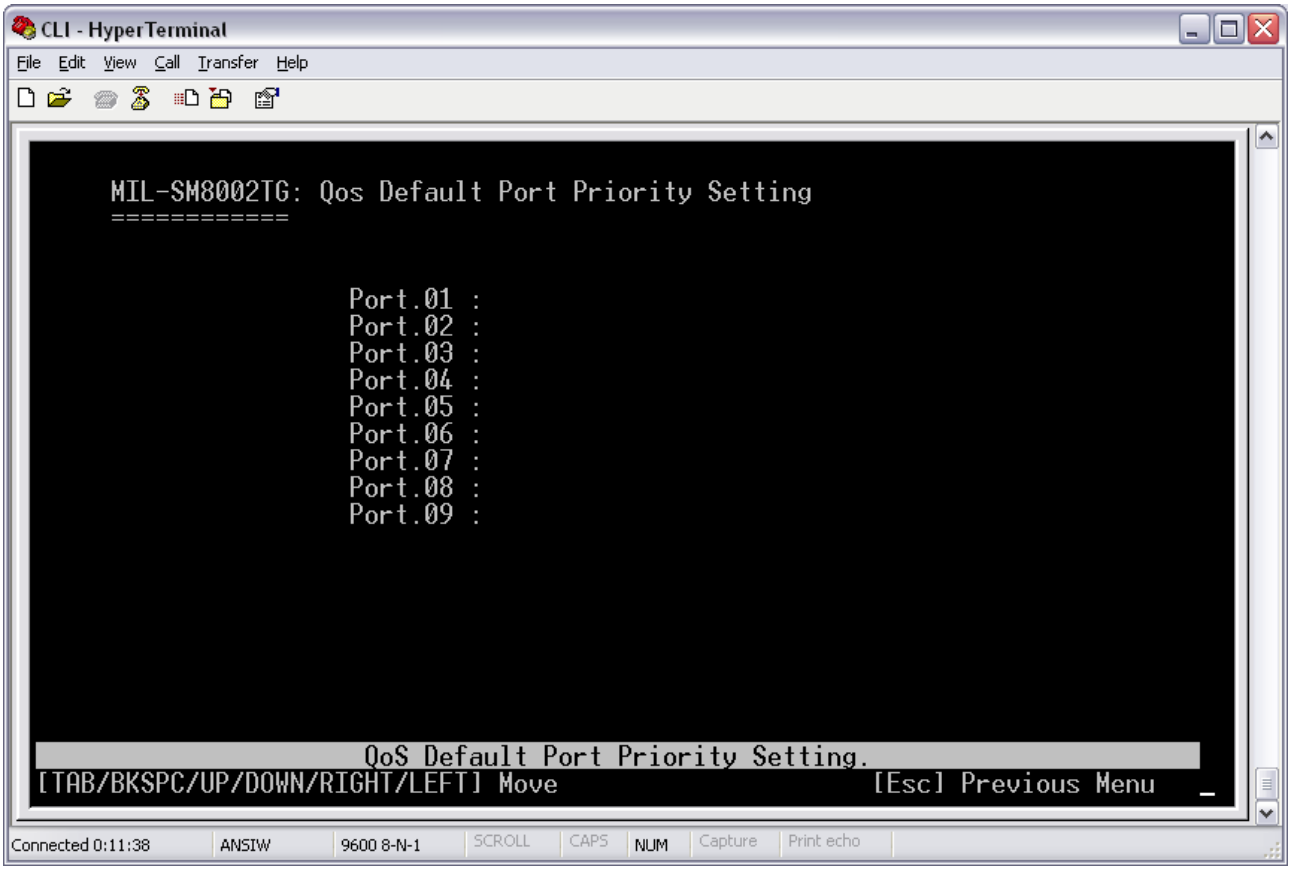
QoS Policy and Priority Type interface

Default Port Priority

Configure per port priority level.

■ **Port 1 ~ 10:** each port has 4 priority levels – High, Middle, Low, and Lowest.

- **Save** the configuration.

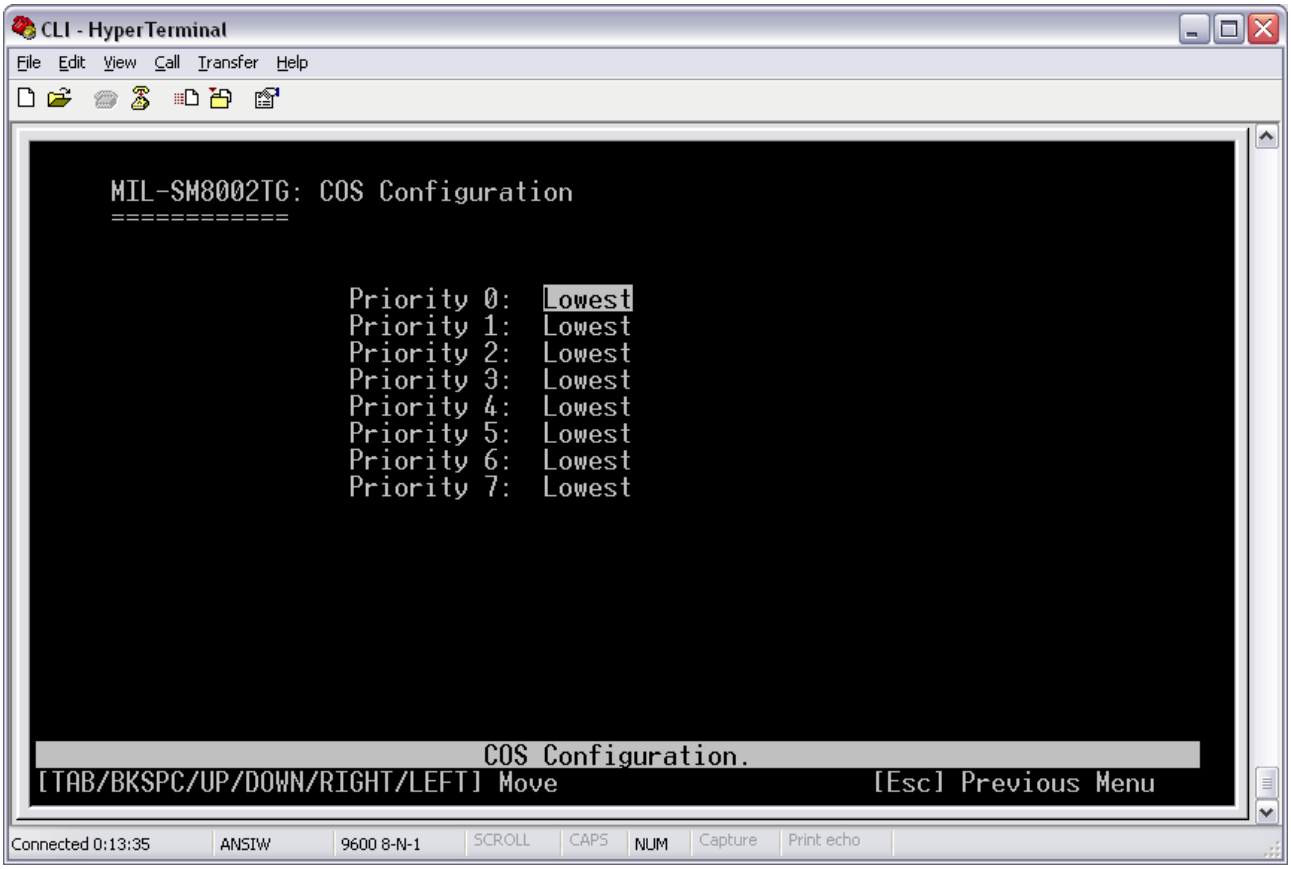


Default Port Priority Setting interface

COS Configuration

Set up the COS priority level.

- **COS priority:**. Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- **Save** the configuration.

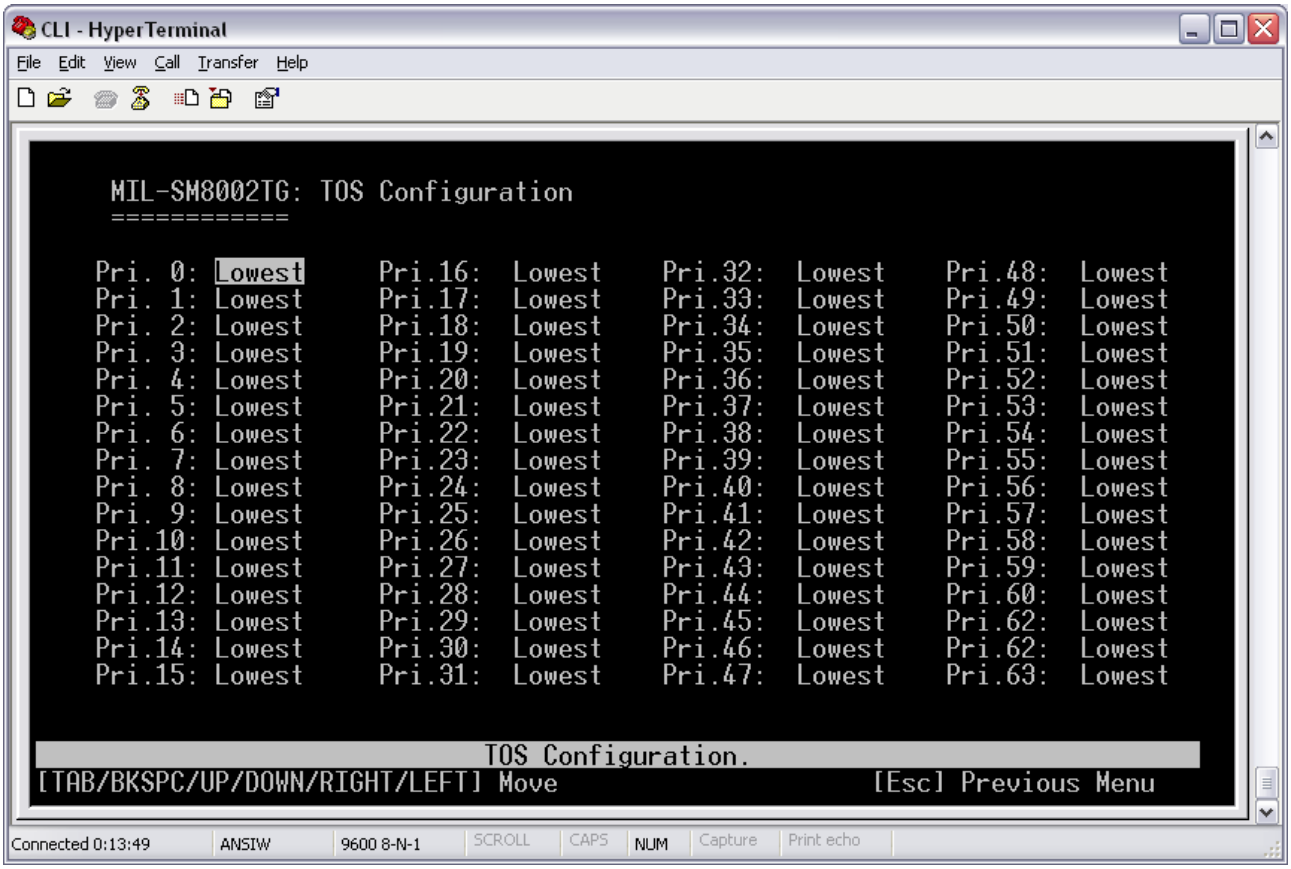


COS Configuration interface

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has 4 types of priority – high, mid, low, and lowest. The default value is “Lowest” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example: user set the TOS level 25 is high. The port 1 is following the TOS priority policy only. When the port 1 packet received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- **Save** the configuration.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: TOS Configuration
Pri. 0: Lowest Pri.16: Lowest Pri.32: Lowest Pri.48: Lowest
Pri. 1: Lowest Pri.17: Lowest Pri.33: Lowest Pri.49: Lowest
Pri. 2: Lowest Pri.18: Lowest Pri.34: Lowest Pri.50: Lowest
Pri. 3: Lowest Pri.19: Lowest Pri.35: Lowest Pri.51: Lowest
Pri. 4: Lowest Pri.20: Lowest Pri.36: Lowest Pri.52: Lowest
Pri. 5: Lowest Pri.21: Lowest Pri.37: Lowest Pri.53: Lowest
Pri. 6: Lowest Pri.22: Lowest Pri.38: Lowest Pri.54: Lowest
Pri. 7: Lowest Pri.23: Lowest Pri.39: Lowest Pri.55: Lowest
Pri. 8: Lowest Pri.24: Lowest Pri.40: Lowest Pri.56: Lowest
Pri. 9: Lowest Pri.25: Lowest Pri.41: Lowest Pri.57: Lowest
Pri.10: Lowest Pri.26: Lowest Pri.42: Lowest Pri.58: Lowest
Pri.11: Lowest Pri.27: Lowest Pri.43: Lowest Pri.59: Lowest
Pri.12: Lowest Pri.28: Lowest Pri.44: Lowest Pri.60: Lowest
Pri.13: Lowest Pri.29: Lowest Pri.45: Lowest Pri.62: Lowest
Pri.14: Lowest Pri.30: Lowest Pri.46: Lowest Pri.62: Lowest
Pri.15: Lowest Pri.31: Lowest Pri.47: Lowest Pri.63: Lowest
TOS Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Esc] Previous Menu
Connected 0:13:49 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

TOS Configuration interface

SNTP Configuration

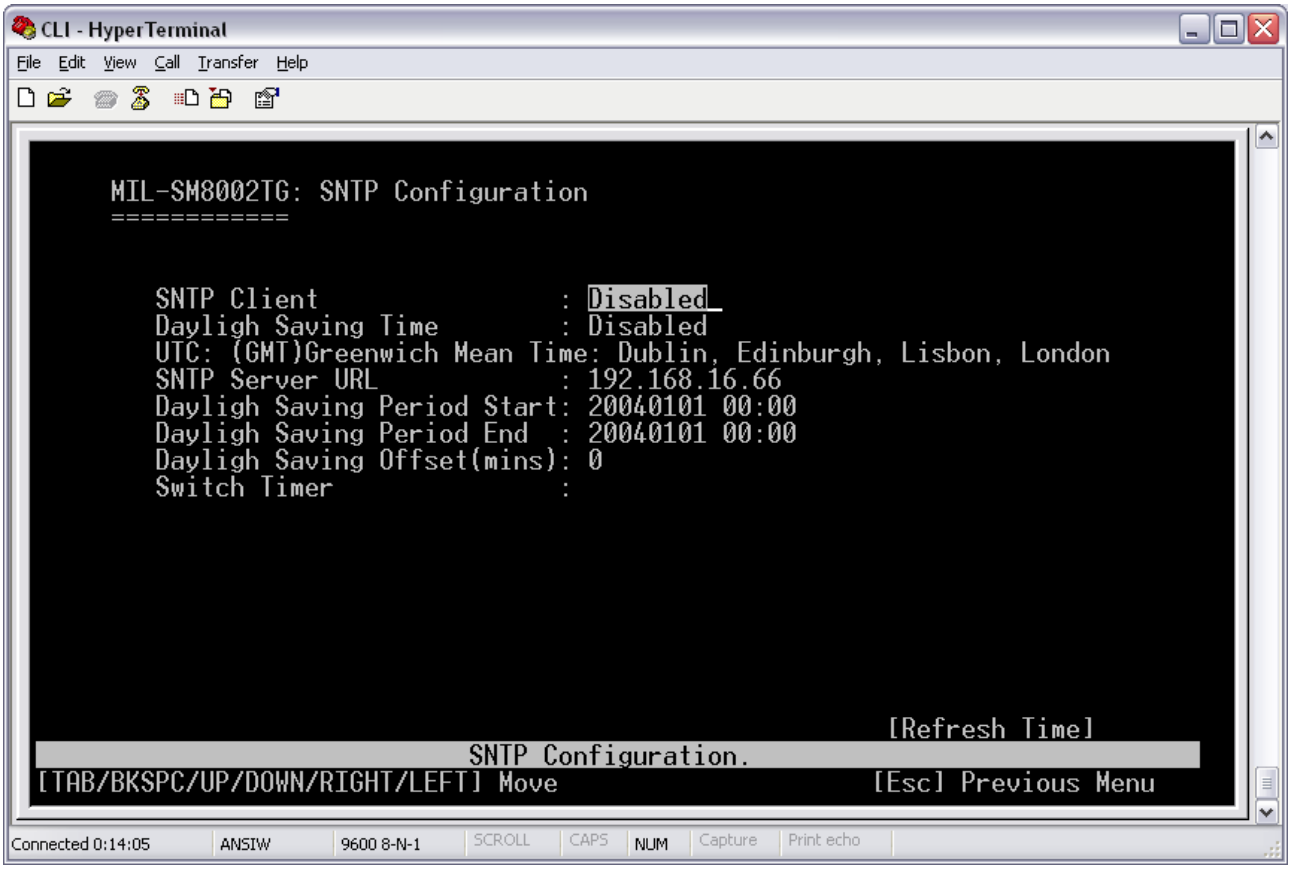
You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period..
3. **UTC Timezone:** set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone	+3 hours	3 pm

2		
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. **SNTP Sever URL:** set the SNTP server IP address.
5. **Daylight Saving Period Start:** set up the Daylight Saving beginning time. Daylight Saving benign time will be different in every year.
6. **Daylight Saving Period End:** set up the Daylight Saving ending time. Daylight Saving ending time will different in every year.
7. **Daylight Saving Offset (mins):** set up the offset time.
8. **Switch Timer:** display the switch current time.



SNTP Configuration interface

IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

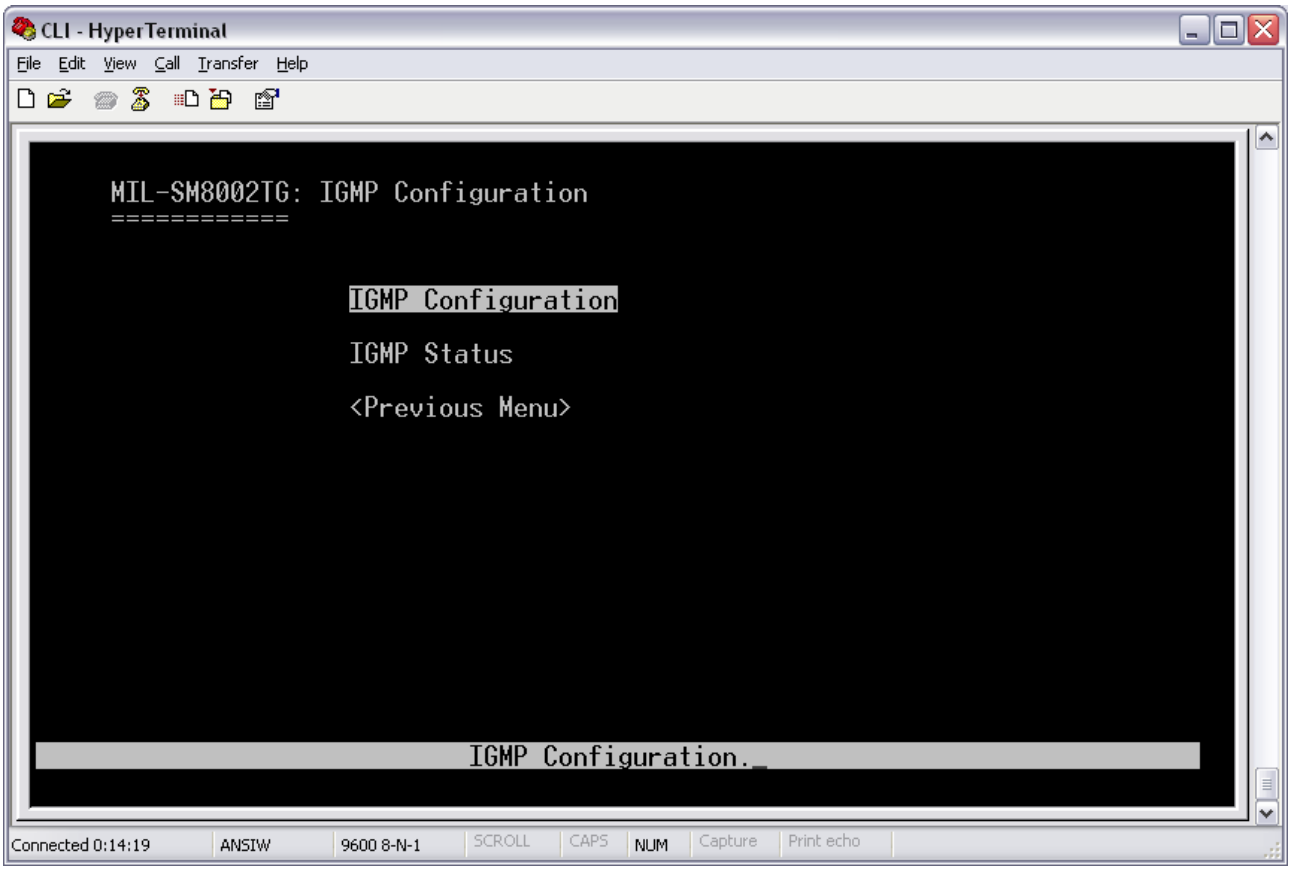
Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.

Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

IGMP Configuration

The switch support IP multicast, you can enable IGMP protocol. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

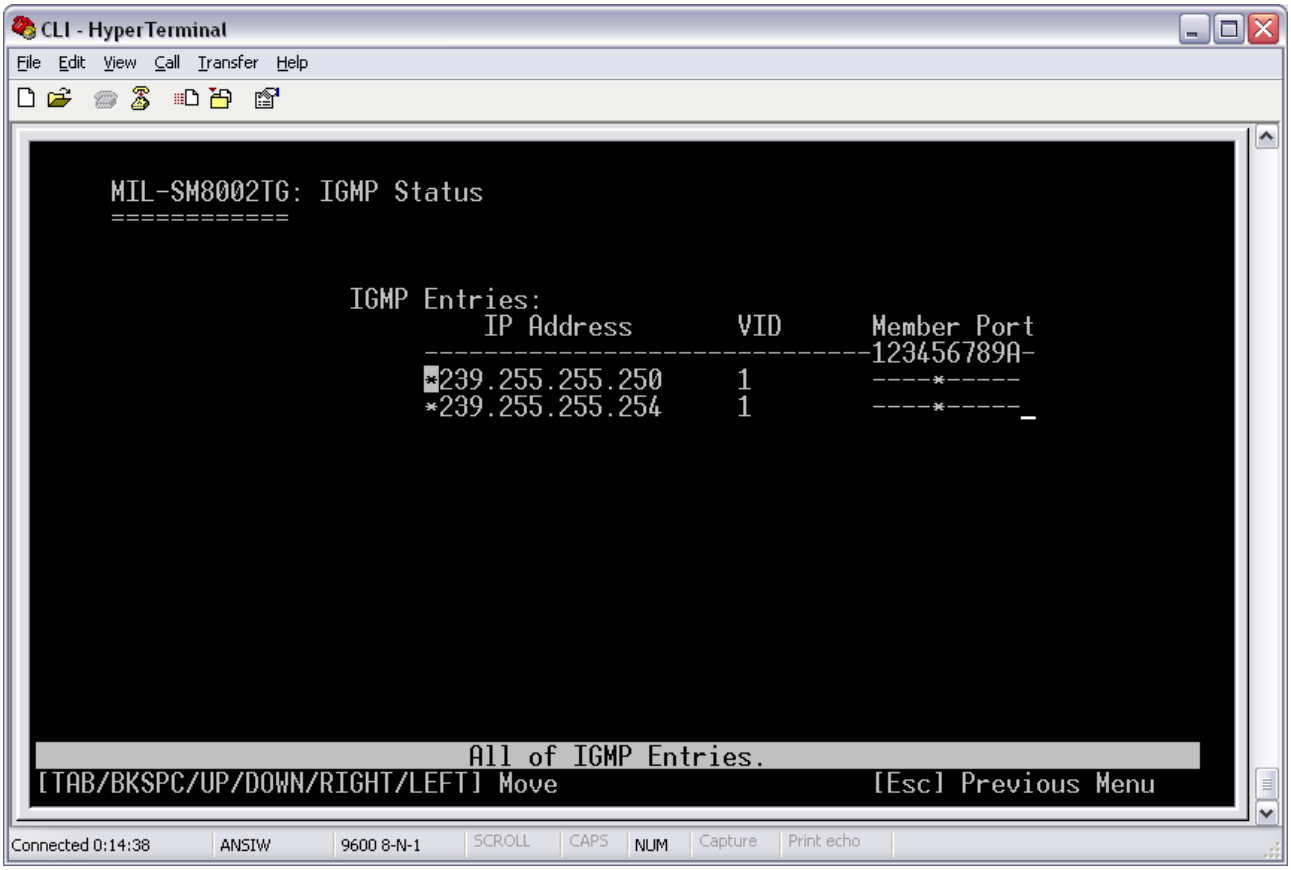
- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be display in IGMP status section.



IGMP Configuration interface

IGMP Status

When you enable the IGMP query you will see the relate information show as following figure.



IGMP Status interface

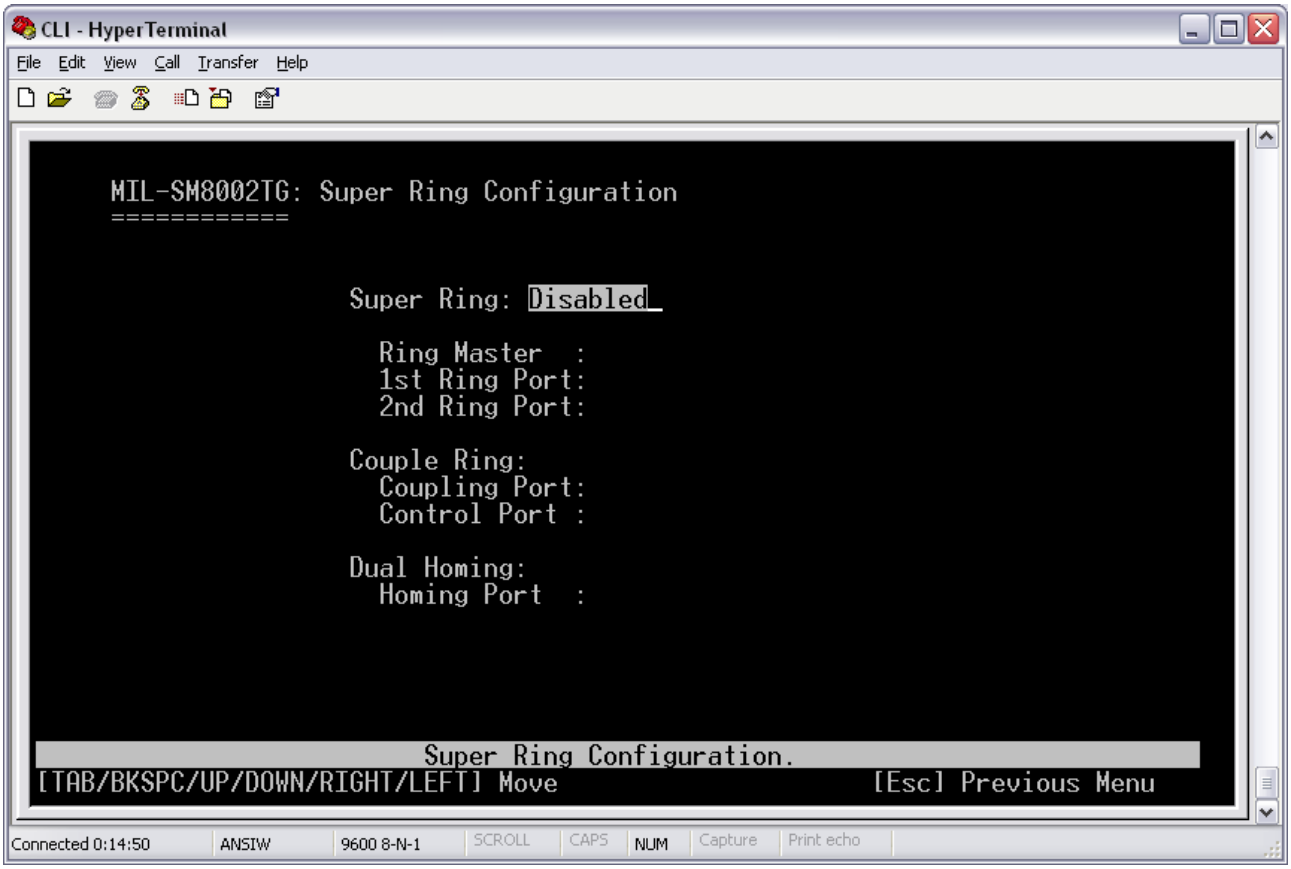
Super ring

Super ring provide a faster redundant recovery than Spanning Tree topology. The action is similar with STP or RSTP, but the algorithms not the same.

In the Super ring topology, every switch should enable super ring function and assign two member ports in the ring. Only one switch in the super ring group would be set as a backup switch that one of two member ports would be blocking, called backup port, and another port is called working port. Other switches are called working switches and their two member ports are called working ports. When the network connection failure, the backup port will automatically become a working port to recovery the failure.
The switch can be set as the ring master or slave. The ring master has the rights to negotiate and place command to other switches in the super ring group. If there are 2 or more switches are in master mode, then software will select the switch with lowest MAC address number as the ring master.

The system also supports the coupling ring that can connect 2 or more super ring group for the redundant backup function.

- **Super ring:** to enable the super ring function.
- **Ring Master:** Enable means the switch is ring master. Disable means the switch is slave.
- **1st & 2nd Ring Ports:** select two ports as the member ports. One port will be working port and one port will be the backup port. The system will automatically decide which port is working port and which port is backup port.
- **Coupling Ring:** to enable the coupling ring function.
- **Coupling port:** select the member port.
- **Control port:** select the switch as the master switch in the coupling ring.

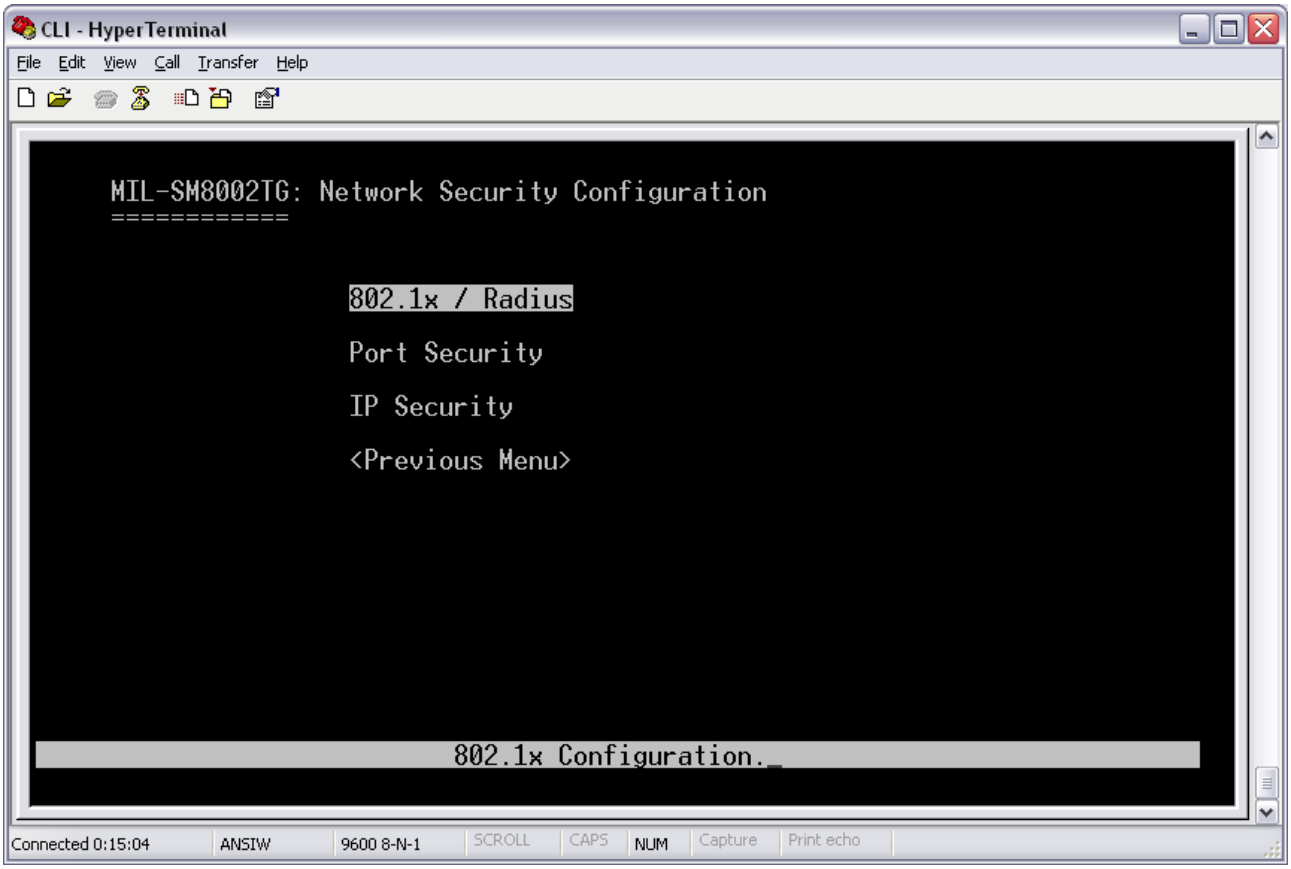


Super ring Interface

[NOTE] When you enable the super ring function, you must disable the RSTP. The super ring function and RSTP function cannot exist at the same time.

Security Configuration

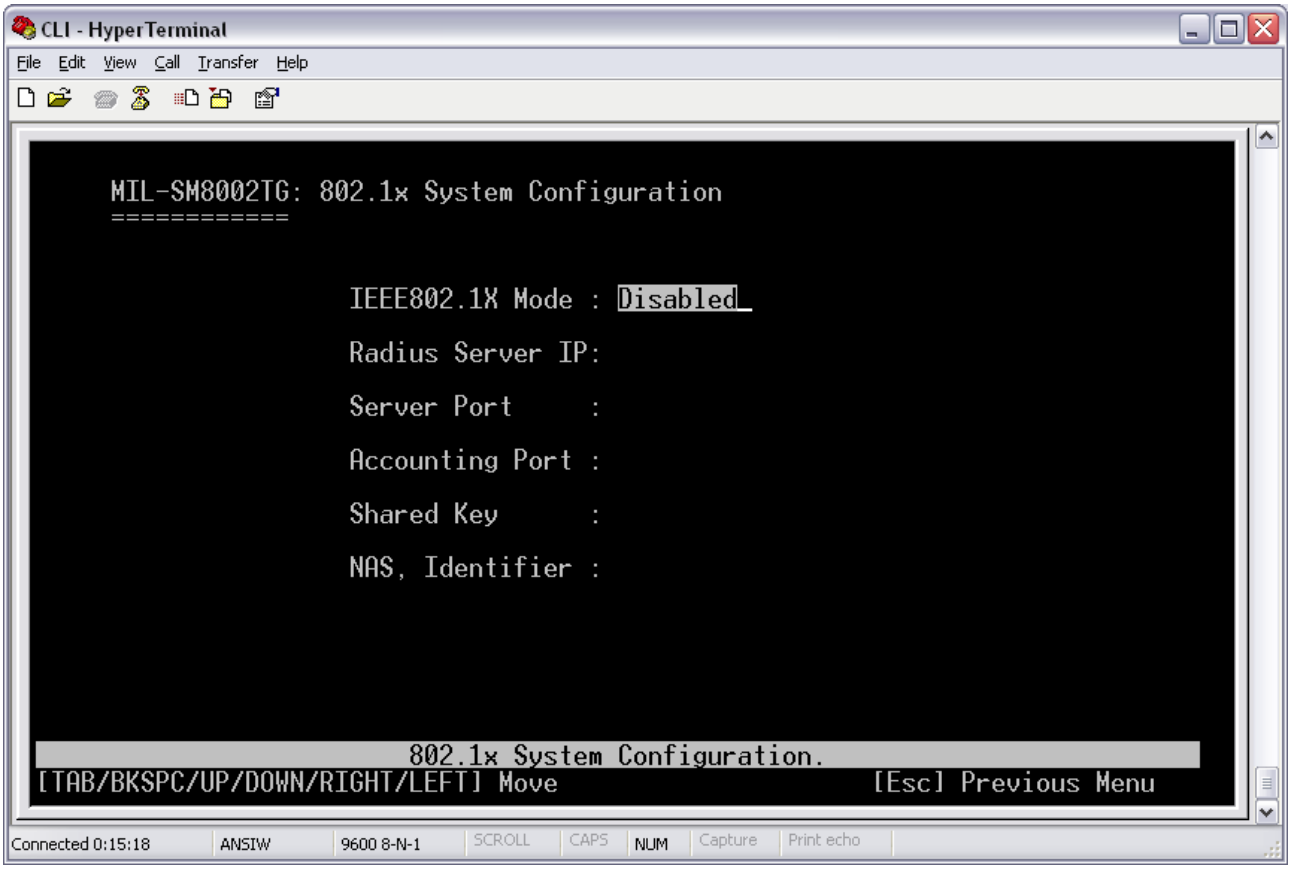
In this section, you can configure 802.1x, IP, and port security.



Security Configuration interface

802.1X/ Radius Configuration

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.



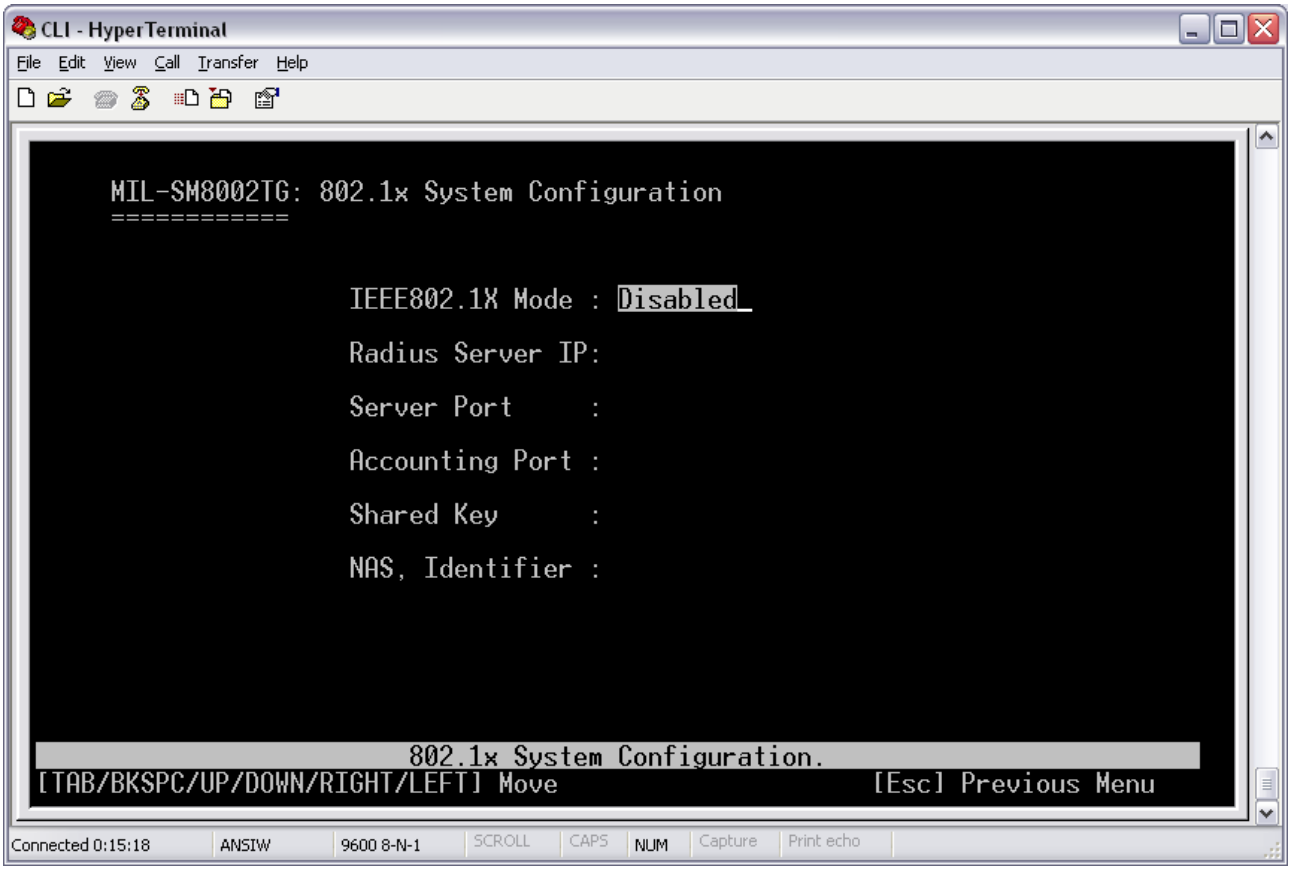
802.1x Configuration interface

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. **IEEE 802.1x mode:** .enable or disable 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.

6. **NAS, Identifier:** set the identifier for the radius client.
7. **Save** the configuration.

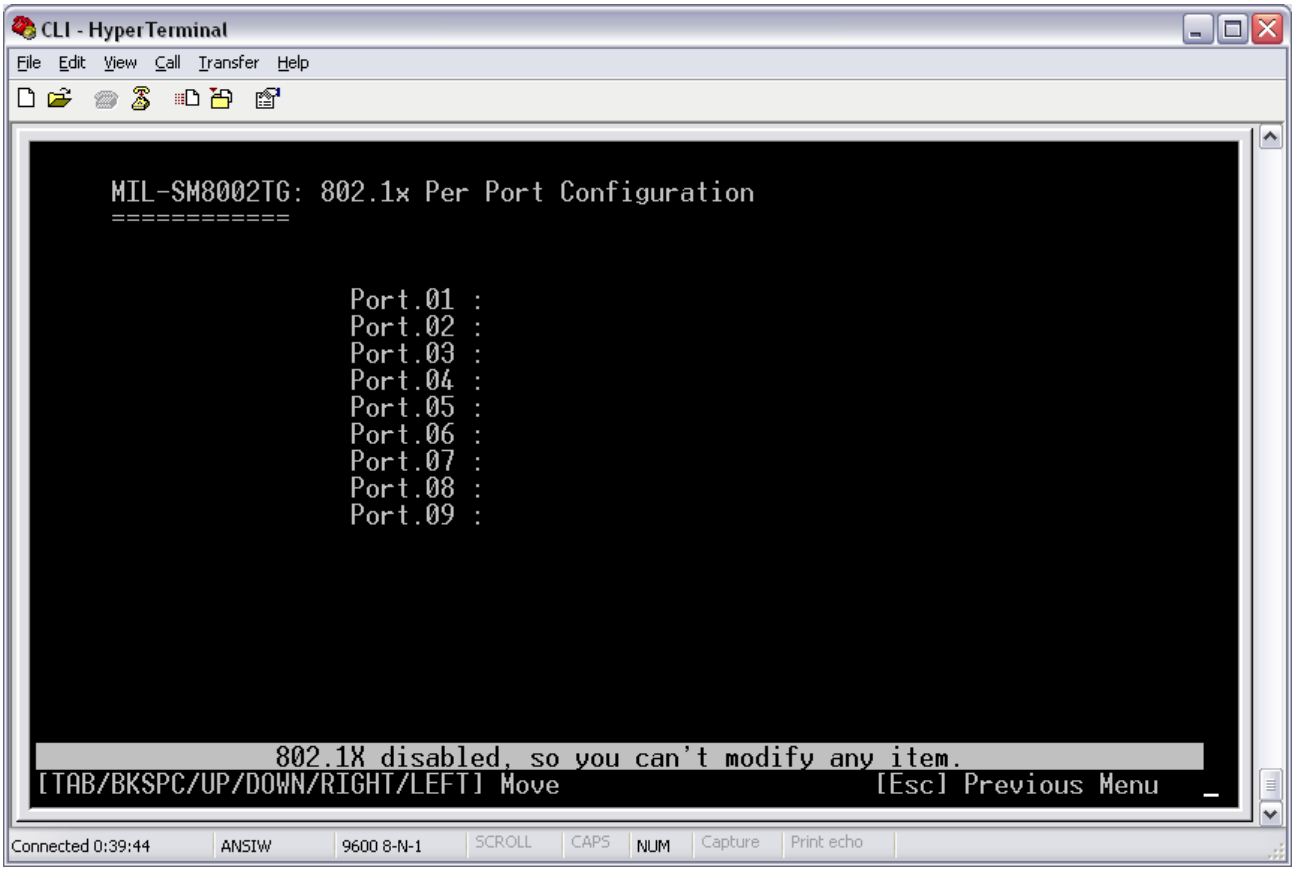


802.1x System Configuration interface

802.1x Per Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use "**Space**" key change the state value.

- **Reject:** the specified port is required to be held in the unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state



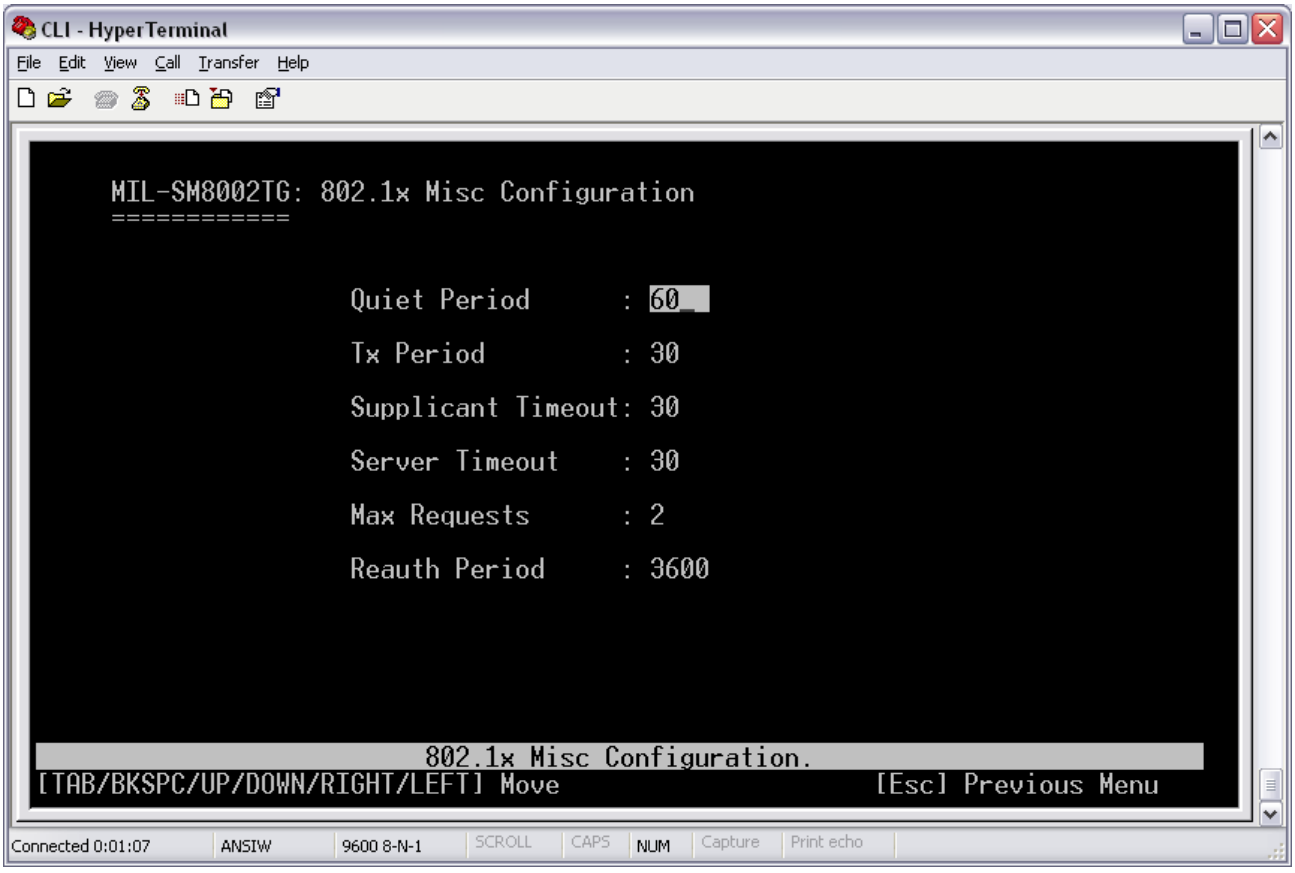
802.1x Per Port Setting interface

Misc Configuration

1. **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.
2. **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch wait for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch wait for a server response to an authentication request.
5. **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which clients connected must be

re-authenticated.

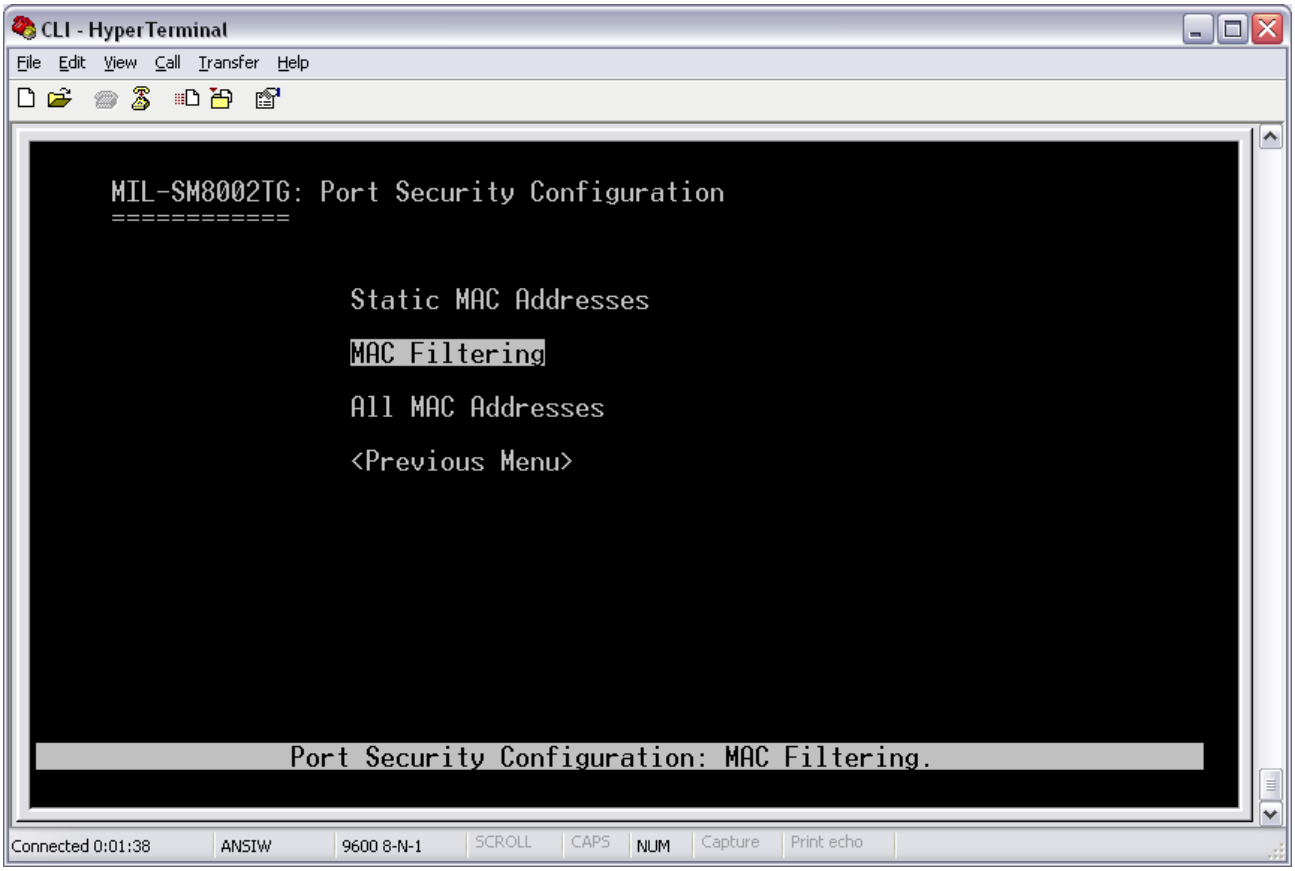
7. Select **<Save>**



802.1x Misc Configuration interface

Port Security

Use the MAC address to ensure the port security.



MAC Address Configuration interface

Static MAC Address

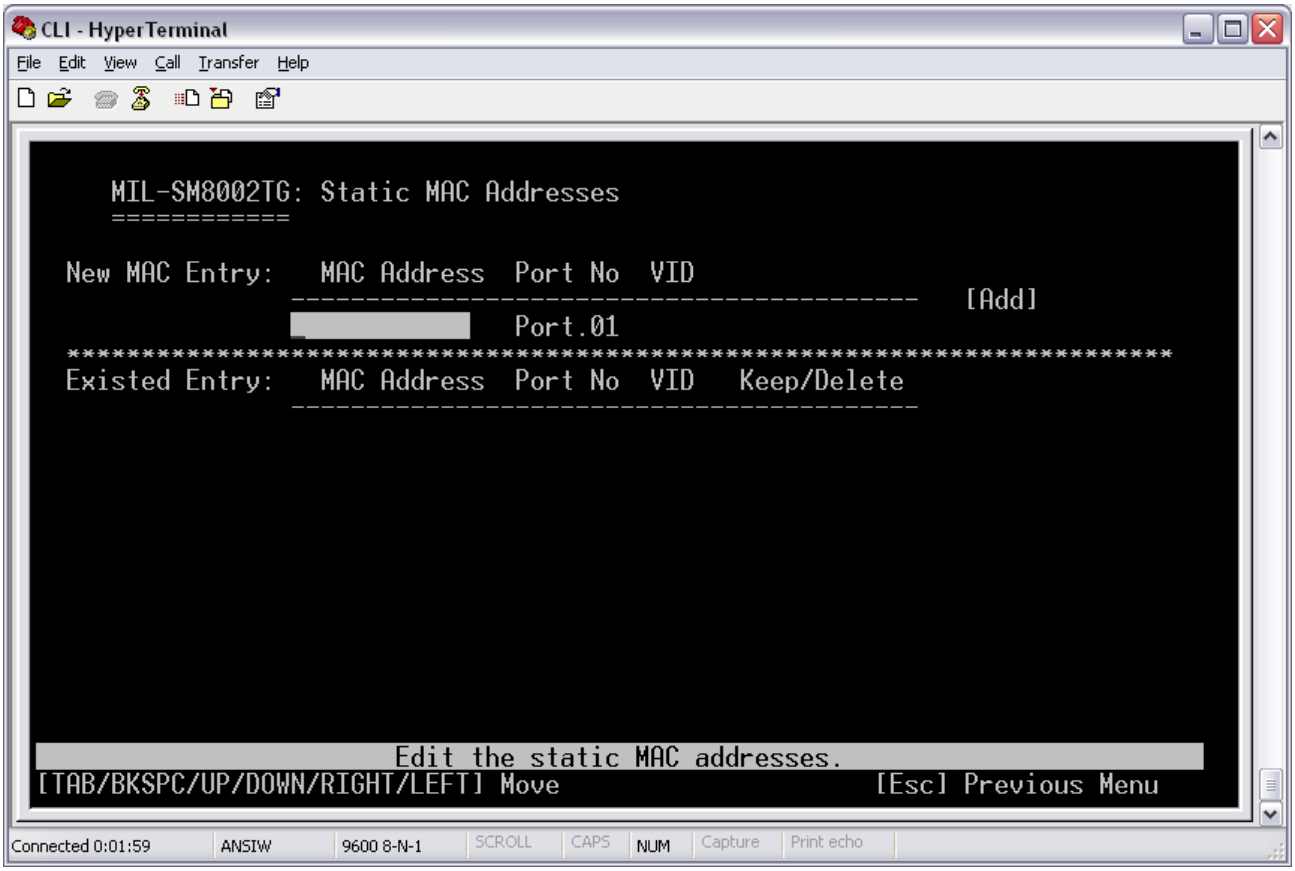
You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

- **Add the Static MAC Address**

You can add static MAC address in switch MAC table.

1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
2. **Port No.:** press "**Space**" key to select the port number.
3. **VID:** enter the Mac address' s VLAD ID, if the Mac address belongs to any VLAN group.

4. Select **<Add>** to save all configure value.
5. **Existed Entry:** you will see the added MAC address information in Exited Entry table. You can delete or keep the added MAC address.



Static MAC Address interface

Filtering MAC Address

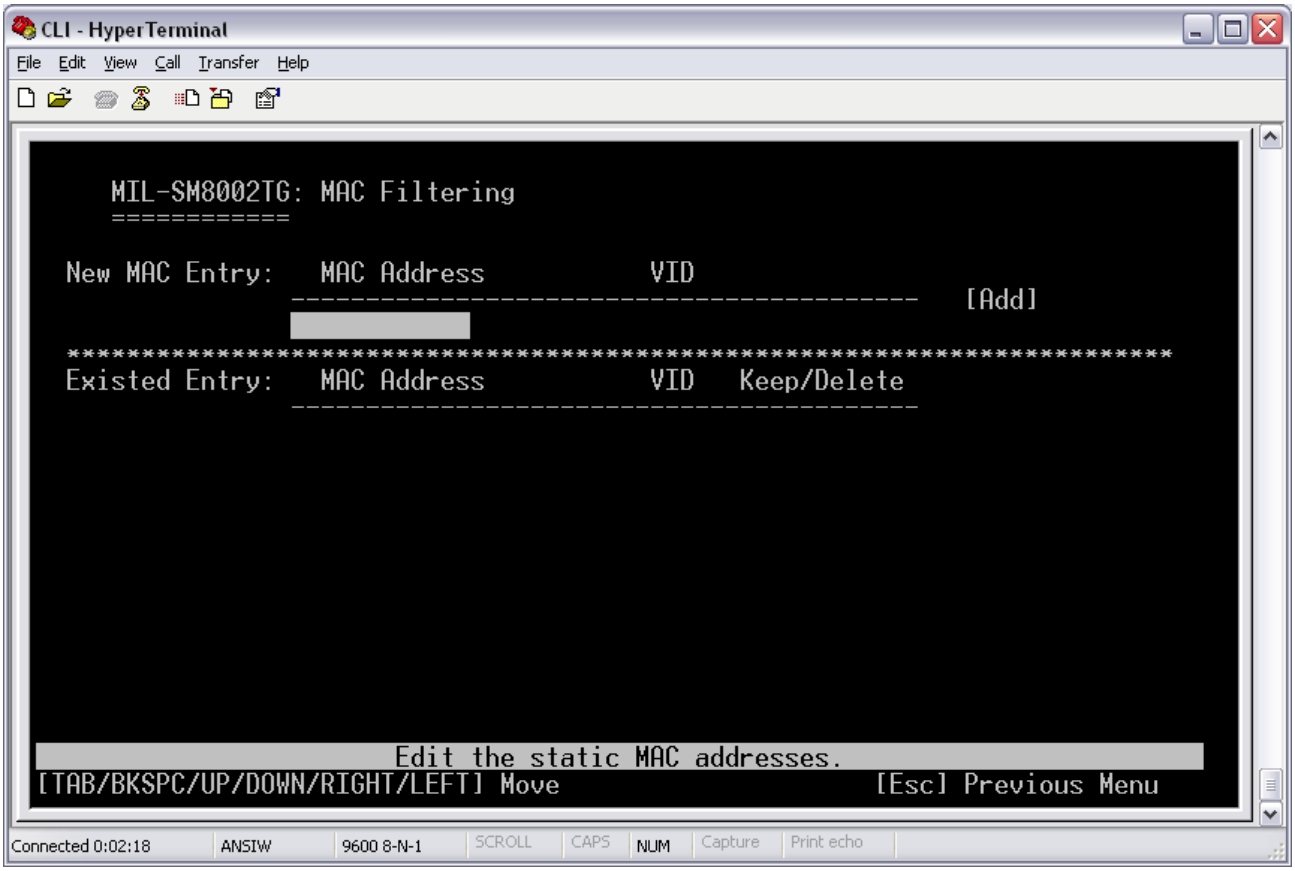
By filtering MAC address, the switch can easily filter pre-configure MAC address and reduce the un-safety. You can add and delete filtering MAC address.

Filtering MAC Address interface

- **Add the Filtering MAC Address**

1. **MAC Address:** Enter the MAC address that you want to filter.
2. **VID:** enter the Mac address's VLAD ID, if the Mac address belongs to any VLAN group.
3. Select **<Add>** to save all configure value.

- **Existed Entry:** you will see the added MAC address information in Exited Entry table. You can delete or keep the added MAC address

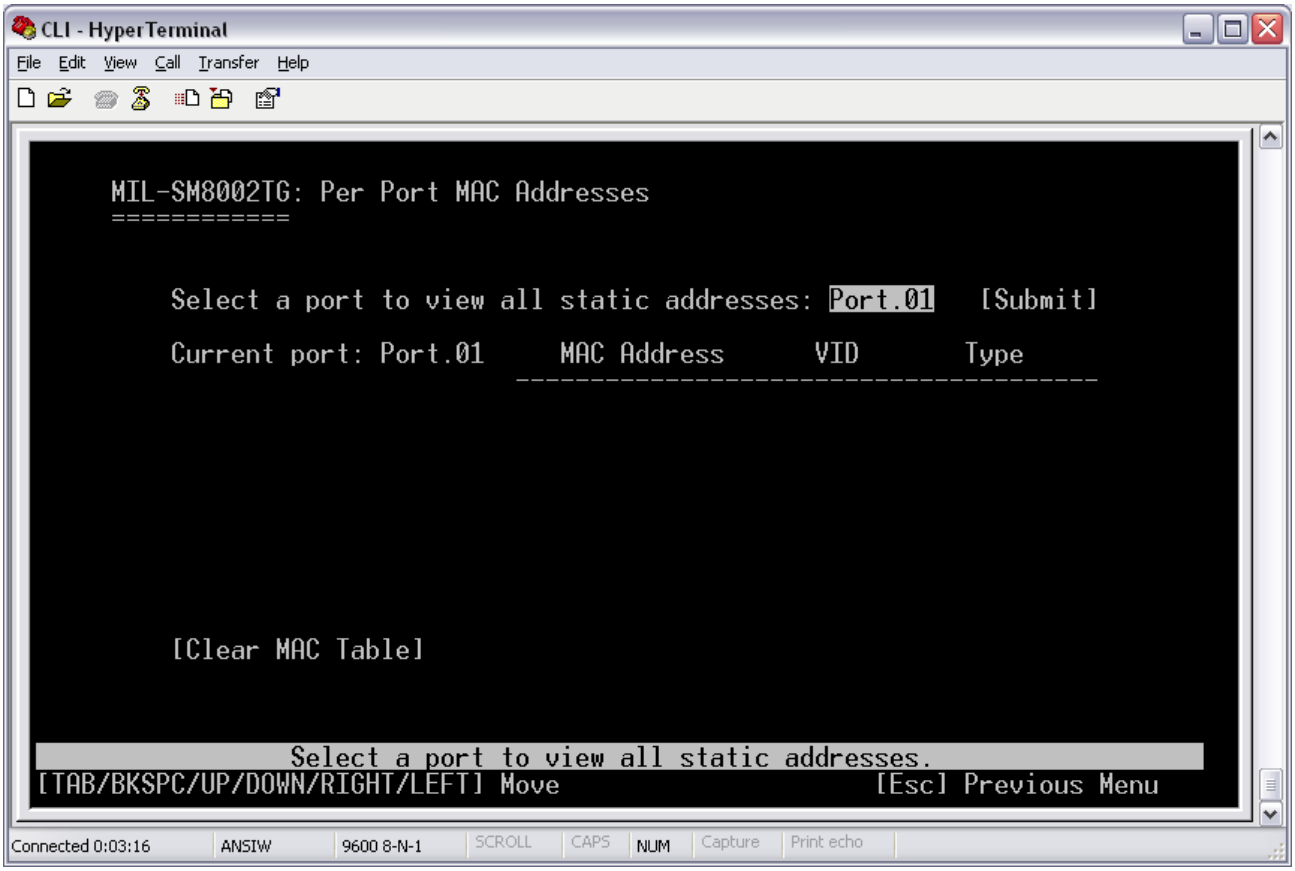


Filtering MAC Address interface

All MAC Address

You can view the port that connected device's MAC address and related devices' MAC address.

1. Select the port and **[Submit]**.



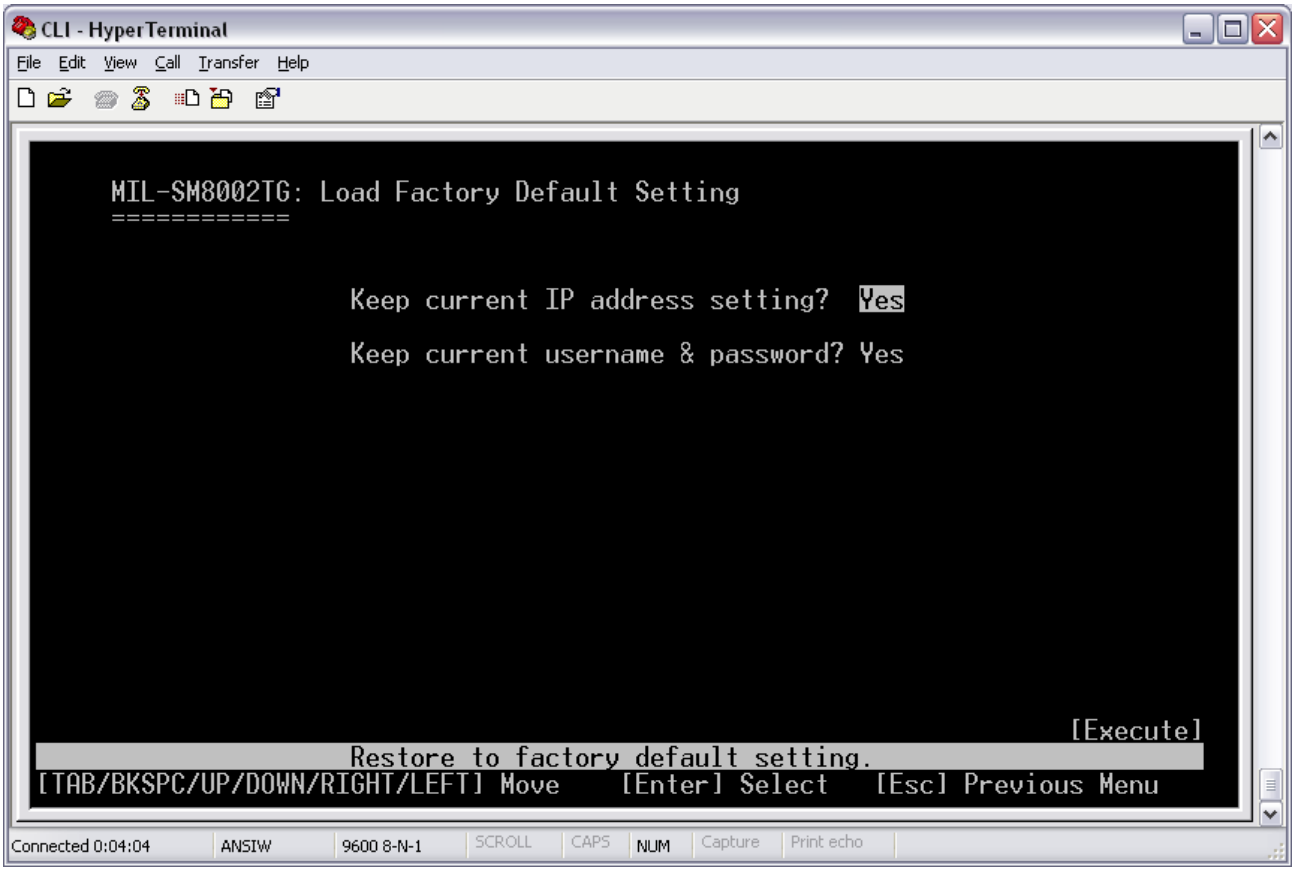
All MAC Address interface

2. The selected port of static MAC address information will display.
3. Select the **[Clear MAC Table]** to clear the current port static MAC address information on screen.

Load Factory Default Setting

Reset switch to default configuration.

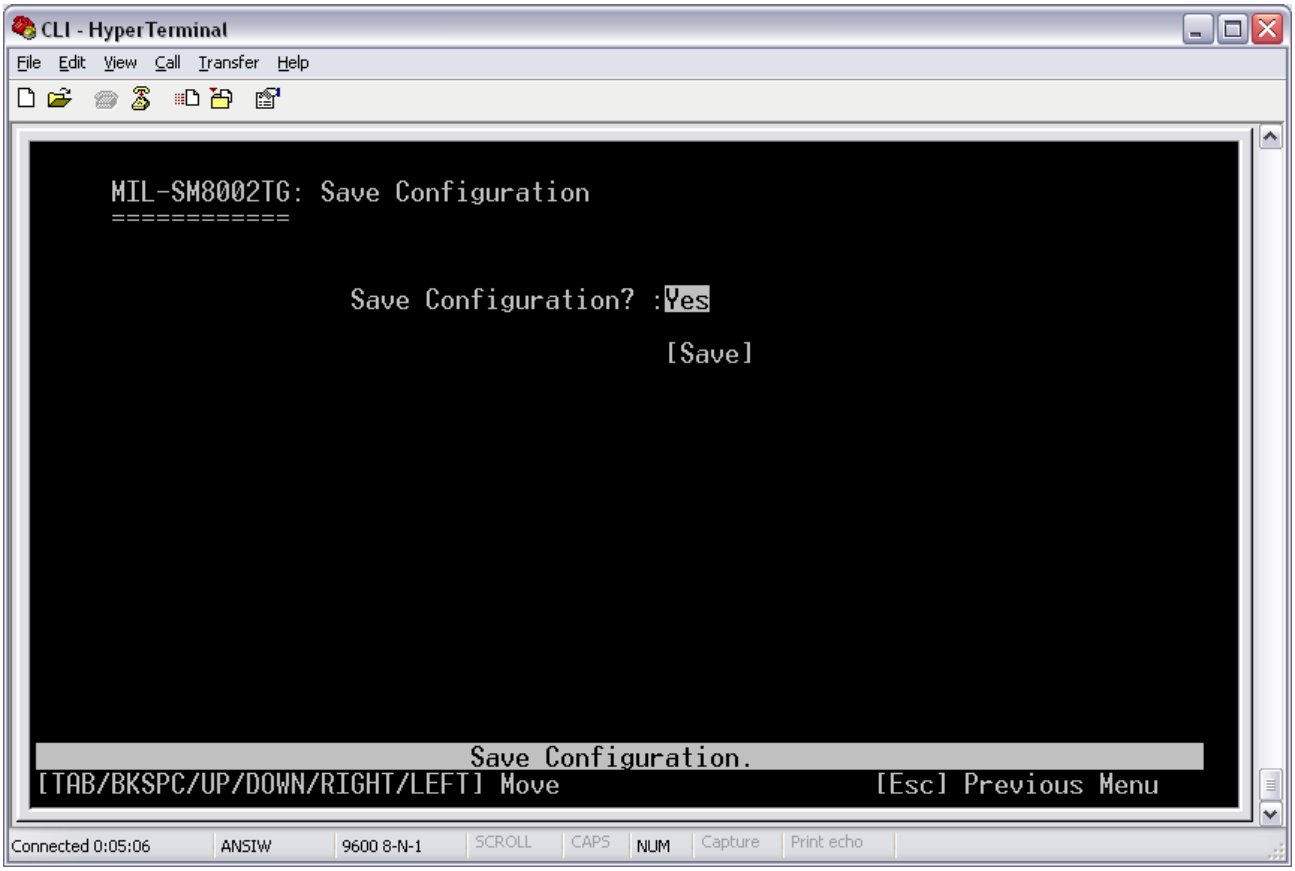
- **Keep current IP address setting?:** you can decided to keep the current IP address or reset to default IP address. Use the **Space** key to mark the selection.
- **Keep current username and password?:** you can decided to keep the current username and password or reset to default username and password. Use the **Space** key to mark the selection.
- After the selection, **[Execute]** to reset.


CLI - HyperTerminal
File Edit View Call Transfer Help
MIL-SM8002TG: Load Factory Default Setting
Keep current IP address setting? Yes
Keep current username & password? Yes
[Execute]
Restore to factory default setting.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move [Enter] Select [Esc] Previous Menu
Connected 0:04:04 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Load Factory Default Setting interface

Save All Configuration

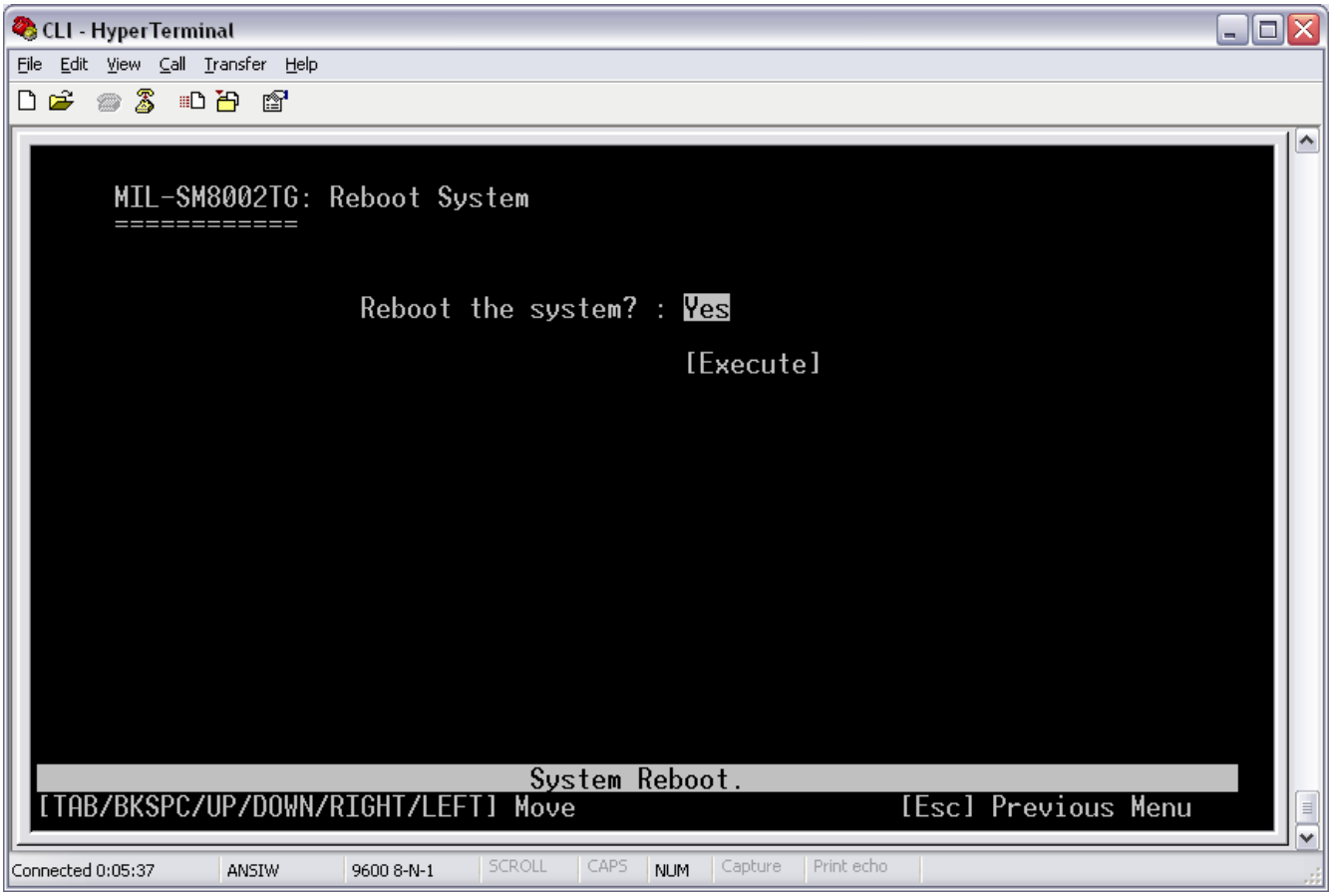
Save all configurations that you have made in the system. To ensure the all configuration will be saved. Use the **Space** key to select the options – **Yes** or **No**. Yes means save all the configurations. No means don't save all configurations. After selected the option, execute the **Save** action to save the configuration.



Save All Configuration interface

Reboot System

Reboot the switch in software reset. Use the **Space** key to select the options – **Yes** or **No**. Yes means reboot the system. No means don't reboot the system. Use **Tab** key move to **[Execute]** action and press **Enter** key to reboot the system.



Reboot System interface

Web-Based Management

Web-Based management offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 5.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

[NOTE]: By default, IE5.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

Preparing for Web Management

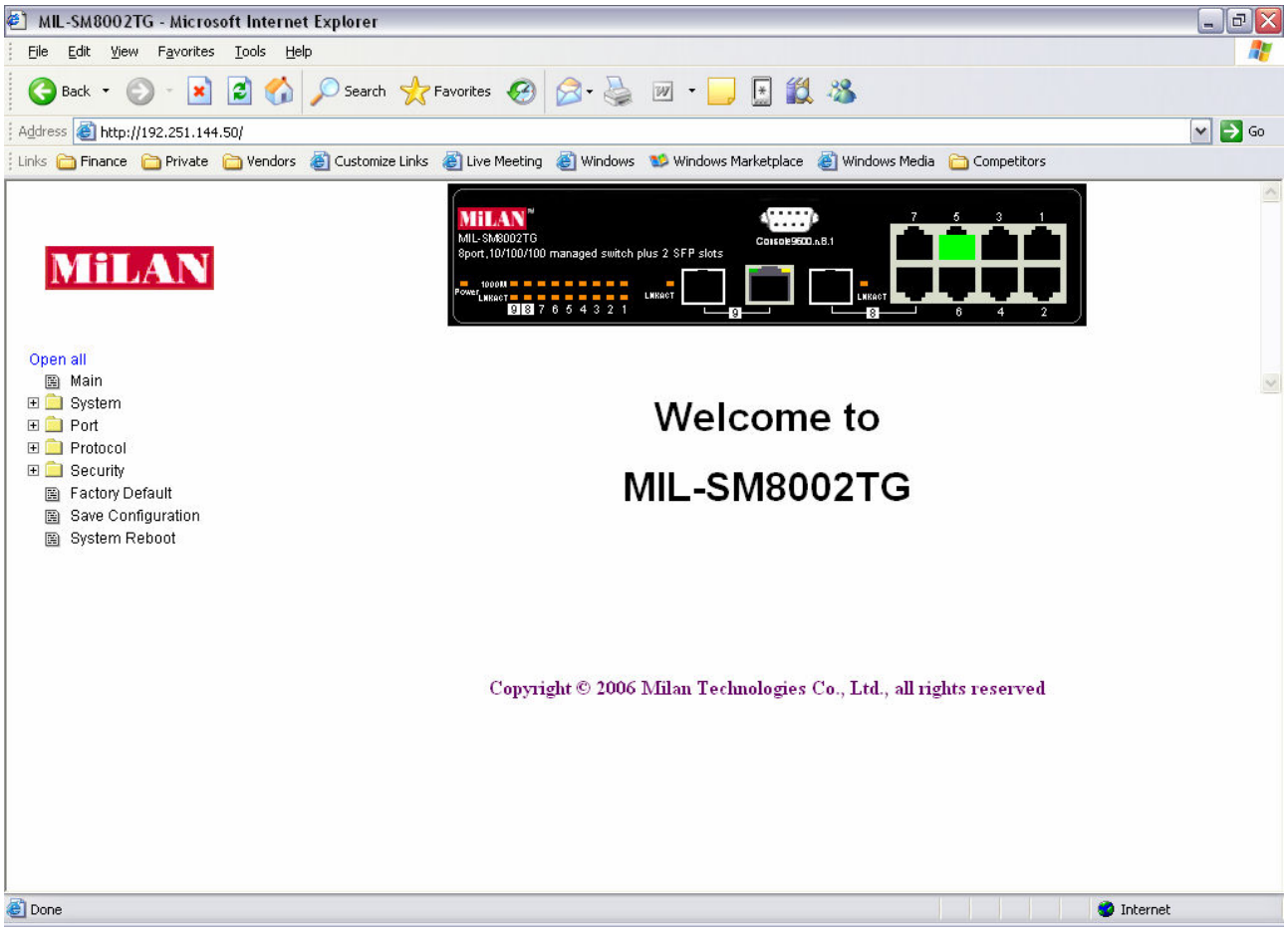
Before use web management, you can use console to login the switch checking the default IP of the Switch. Please refer to **Console Management** Chapter for console login. If you need change IP address in first time, you can use console mode to modify it. The default value is as below:

IP Address:	**192.168.1.77**
Subnet Mask:	**255.255.255.0**
Default Gateway:	**192.168.1.254**
User Name:	**root**
Password:	**root**

System Login

1. Launch the Internet Explorer.

2. Type http:// and the IP address of the switch. Press “**Enter**”.
3. The login screen appears.
4. Key in the user name and password. The default user name and password is “**root**”.
5. Click “**Enter**” or” **OK**”, then the home screen of the Web-based management appears.



Main interface

System Information

You can assign the system name and location and view the system information.

System Name: assign the name of switch. The maximum length is 64 bytes.

- **System Name:** assign the system name of the switch. The maximum length is 64

bytes.

- **System Location:** assign the switch physical location. The maximum length is 64 bytes.
- **System Description:** display the description of switch. Read only cannot be modified.
- **Firmware Version:** display the switch's firmware version.
- **Kernel Version:** display the kernel software version.
- **Hardware version:** display the switch hardware version.
- **MAC Address:** display the unique hardware address assigned by manufacturer (default).

System Information interface

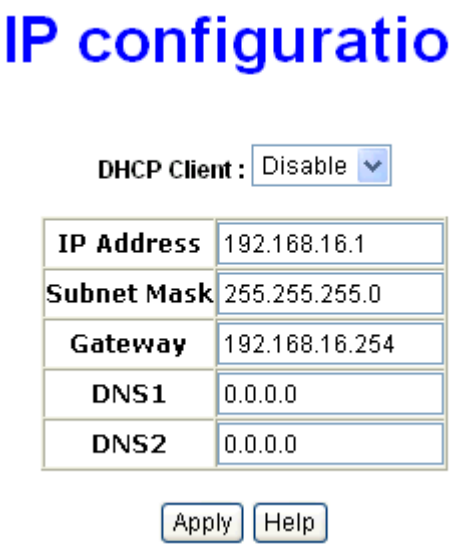
IP Address

User can configure the IP Settings and DHCP client function, than clicks Apply button.

After reset the IP address, you must reboot the switch.

- **DHCP:** disable or enable the DHCP client function.
- **IP Address:** assign the switch IP address. The default IP is 192.168.1.77.
- **Subnet Mask:** assign the switch IP subnet mask.

- **Gateway:** assign the switch gateway. The default value is 192.168.1.254.
- **DNS1:** Short for Domain Name Server an Internet service that translates domain name into IP addresses. Because domain name are alphabetic, they're easier to remember. The Internet is based on IP address. Every time you use a domain name , therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name **www.net.com** might translate to **192.168.1.1**.
- **DNS2:** The backup for DNS1. When the DNS1 cannot function, the DNS2 can replace DNS1 immediately.



IP configuration interface

DHCP Configuration

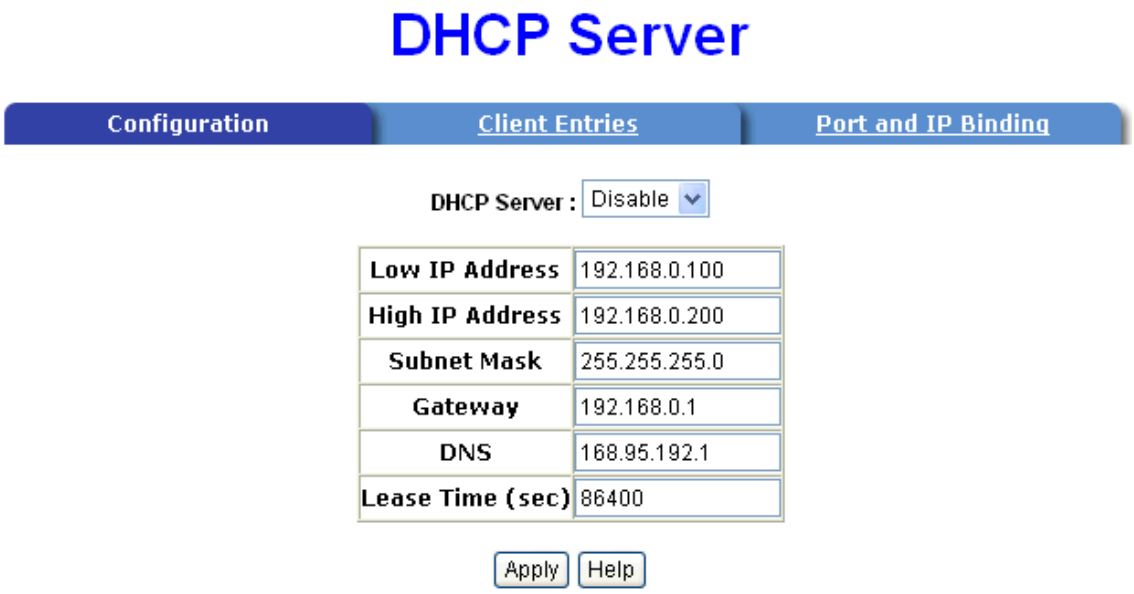
It short for Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration

because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Server Configuration

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network.
- **Low IP Address:** the dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.169.1.0 ~ 192.168.1.30. 192.168.1.0 will be the Low IP address.
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.169.1.0 ~ 192.168.1.30. 192.168.1.30 will be the High IP address.
- **Subnet Mask:** the dynamic IP assign range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.



DHCP Server Configuration interface

DHCP Client Entries

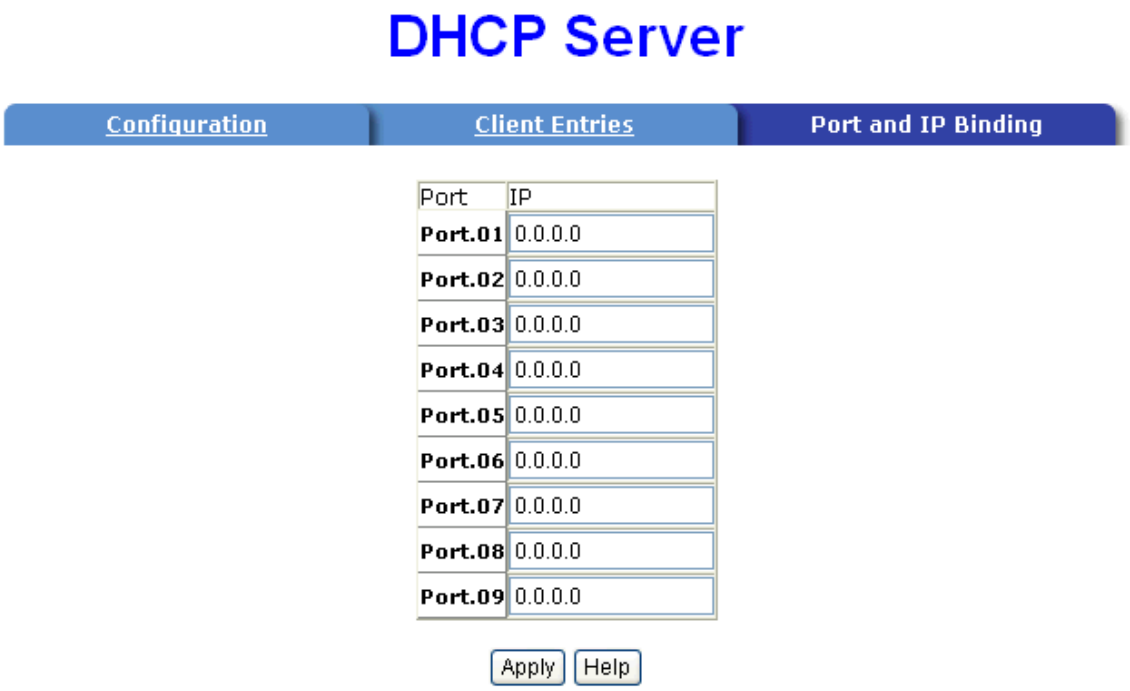
When the DHCP server function is active, the system will collect the DHCP client information and display in here.

DHCP Client Entries interface

Port and IP Bindings

You can assign the specific IP address that is the IP in dynamic IP assign range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before to the connected

device.

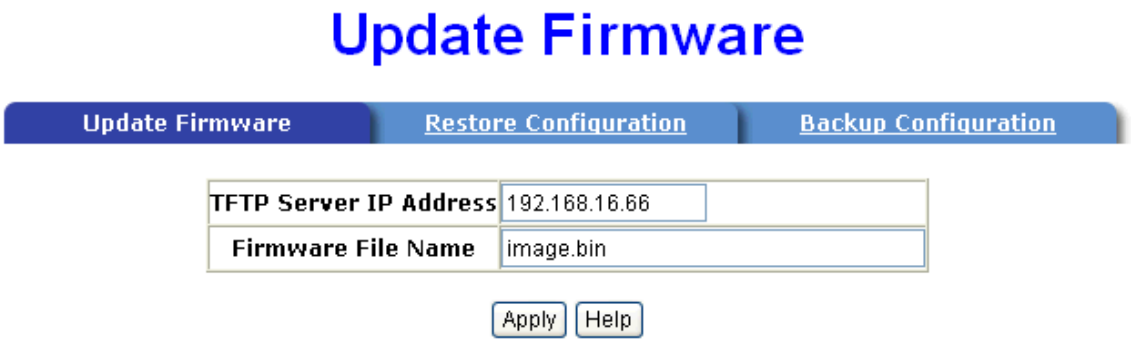


Port and IP Bindings interface

Update Firmware

It provides the functions to allow a user to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

1. **TFTP Server IP Address:** fill in your TFTP server IP.
2. **Firmware File Name:** the name of firmware image.
3. Click Apply.

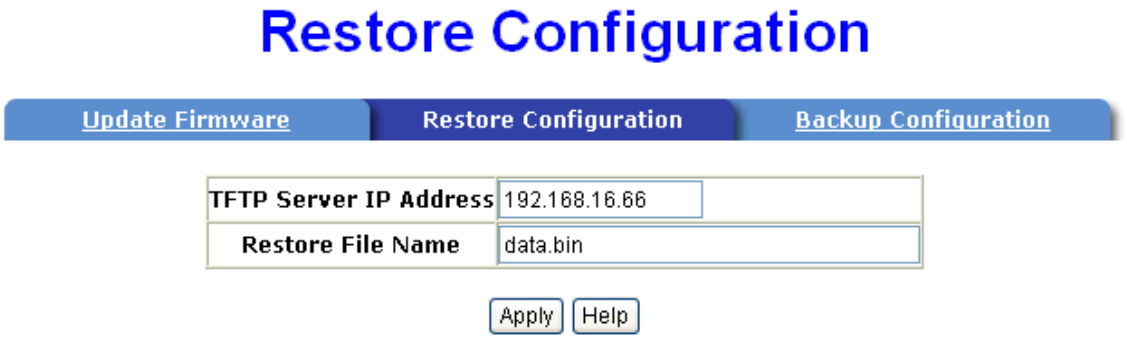


Update Firmware interface

Restore Configuration

You can restore EEPROM value from TFTP server, but you must put back image in TFTP server, switch will download back flash image.

1. **TFTP Server IP Address:** fill in the TFTP server IP.
2. **Restore File Name:** fill in the correct restore file name.
3. Click Apply.

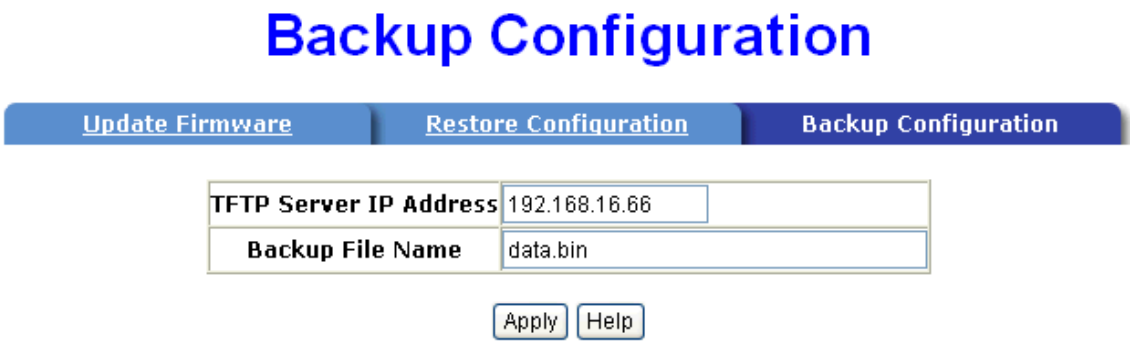


Restore Configuration interface

Backup Configuration

You can save current EEPROM value from the switch to TFTP server, then go to the TFTP restore configuration page to restore the EEPROM value.

1. **TFTP Server IP Address:** fill in the TFTP server IP
2. **Backup File Name:** fill the file name
3. Click Apply.



Backup Configuration interface

System Log Configuration

Configuring the system event mode that want to be collected and system log server IP.

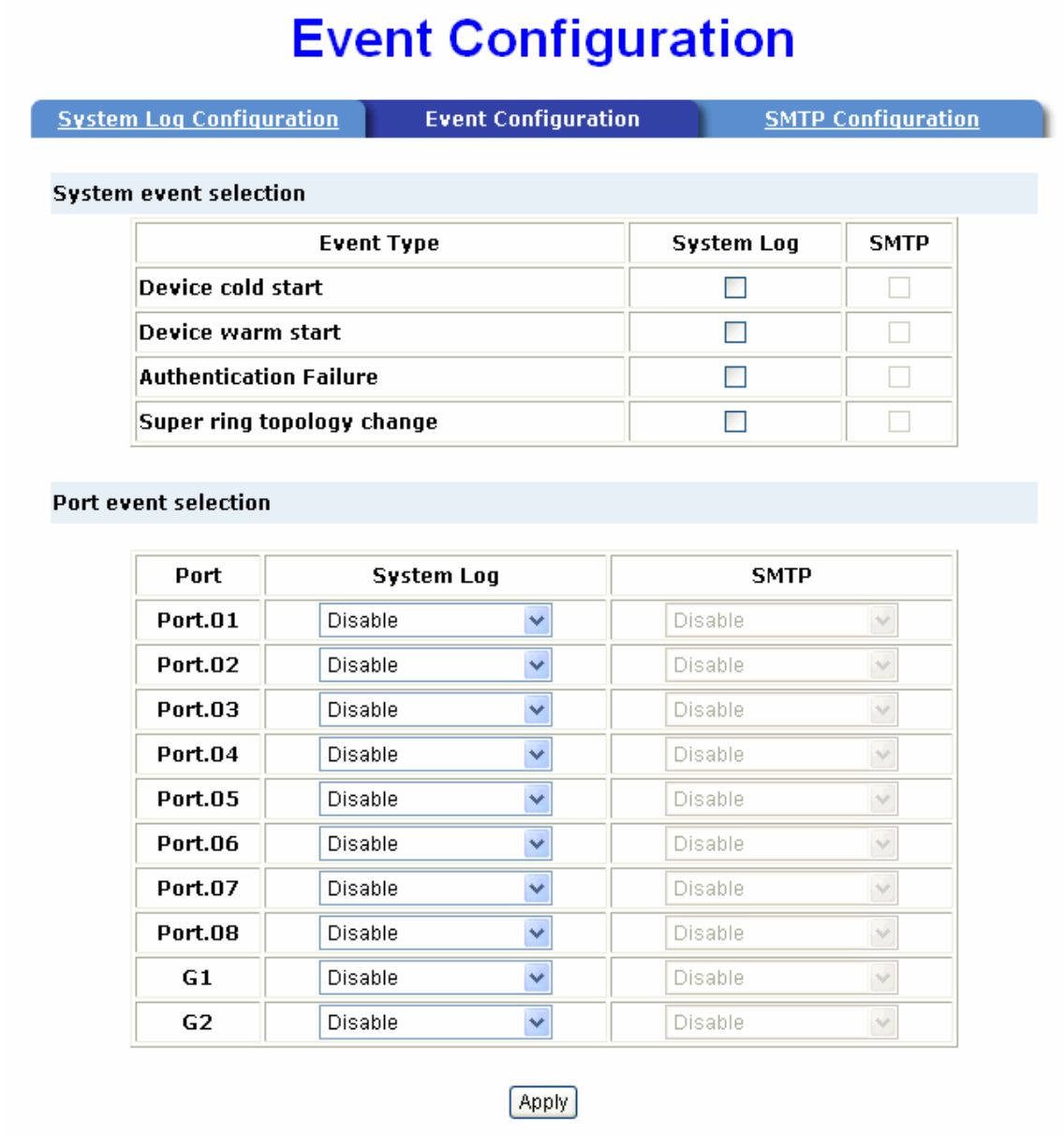
1. **System Log Client Mode:** select the system log mode – client only, server only, or both S/C.
2. **System Log Server IP Address:** assigned the system log server IP.
3. Click Reload to refresh the events log.
4. Click Clear to clear all current events log.

System Log Configuration interface

Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the log information. Also, per port log and SMTP events can be selected. After configure, Click Apply.

- **System event selection:** 4 selections – Device cold start, Power status, SNMP Authentication Failure, and Super ring topology change. Mark the checkbox to select the event. When selected events occur, the system will produce the logs.
  - **Device cold start:** when the device executes cold start action, the system will produce a log event.
  - **Device warm start:** when the device executes warm start, the system will produce a log event.
  - **Authentication Failure:** when the SNMP authentication fails, the system will produce a log event.
  - **Super Ring topology change:** when the Super ring topology has changed, the system will produce a log event.



Event Configuration interface

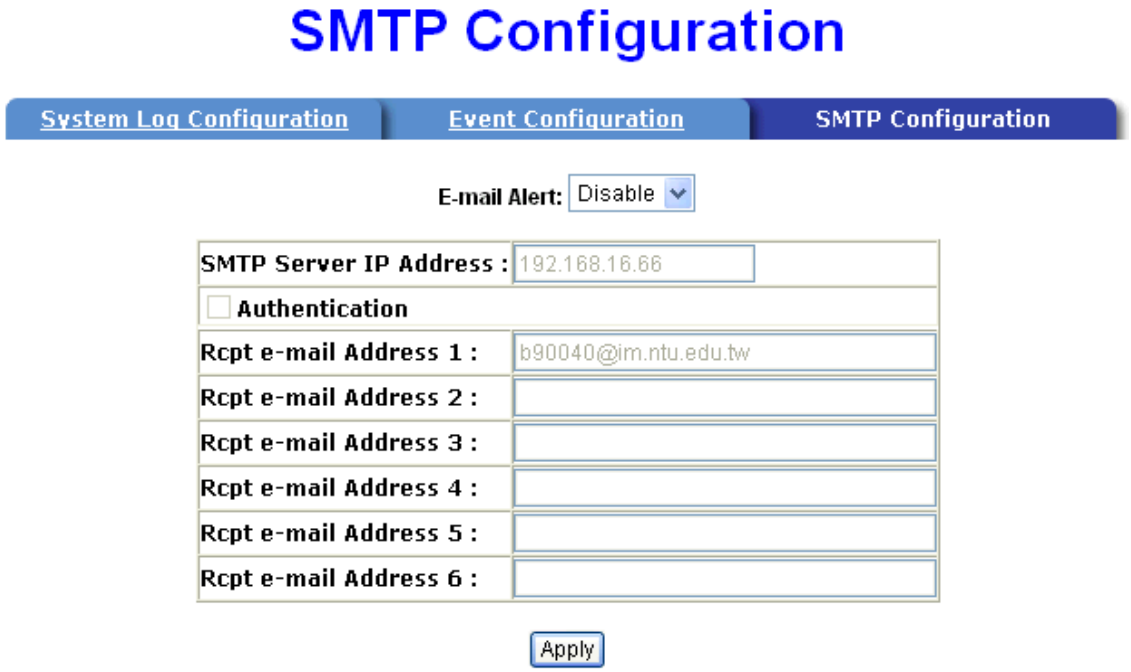
- **Port event selection:** select the per port events and per port SMTP events. It has 3 selections – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected.
  - **Link UP:** the system will produce a log message when port connection is up only.
  - **Link Down:** the system will produce a log message when port connection is down only.

- **Link UP & Link Down:** the system will produce a log message when port connection is up and down.

SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address.
3. **Authentication:** mark the check box to enable and configure the email account and password for authentication.
4. **Mail Account:** set up the email account to receive the alert. Ex: johnadmin@123.com. The email account must exist on the mail server, which you had set up in **SMTP Server IP Address** column.
5. **Password:** The email account password.
6. **Confirm Password:** reconfirm the password.
7. **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
8. Click Apply.



SMTP Configuration interface

Security Manager

You can change web management login user name and password.

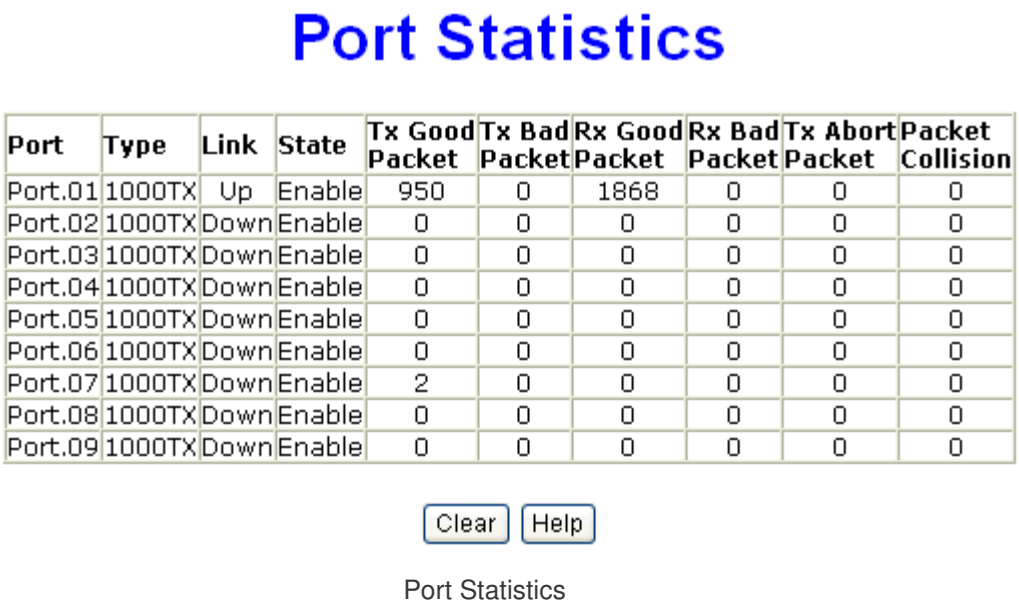
1. **User name:** type the new user name. The default is “root”
2. **Password:** type the new password. The default is “root”
   Confirm password: retype the new password.
3. Click Apply.

Security Manager interface

Port Statistics

The following information provides a view of the current port statistic information.

Click Clear button to clean all counts.


Port Statistics
Port Type Link State Tx Good Packet Tx Bad Packet Rx Good Packet Rx Bad Packet Tx Abort Packet Packet Collision
Port.01 1000TX Up Enable 950 0 1868 0 0 0
Port.02 1000TX Down Enable 0 0 0 0 0 0
Port.03 1000TX Down Enable 0 0 0 0 0 0
Port.04 1000TX Down Enable 0 0 0 0 0 0
Port.05 1000TX Down Enable 0 0 0 0 0 0
Port.06 1000TX Down Enable 0 0 0 0 0 0
Port.07 1000TX Down Enable 2 0 0 0 0 0
Port.08 1000TX Down Enable 0 0 0 0 0 0
Port.09 1000TX Down Enable 0 0 0 0 0 0
Clear
Help

Port Statistics

Port Control

In Port control, you can view every port status that depended on user setting and the negotiation result.

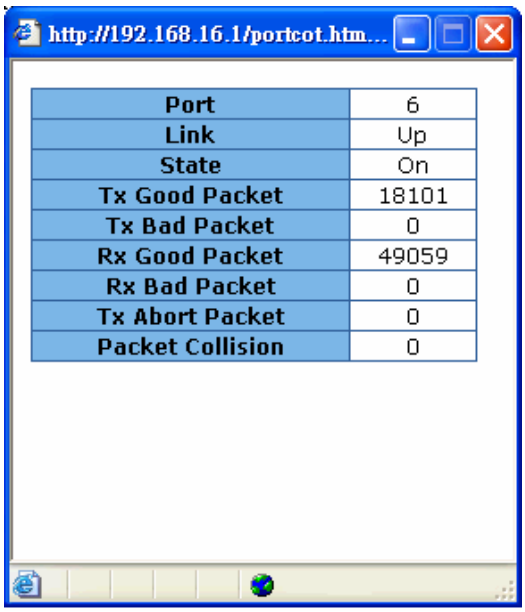
1. **Port:** select the port that you want to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
3. **Negotiation:** set auto negotiation status of port.
4. **Speed:** set the port link speed.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set flow control function is **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Disable**.
7. Click Apply.

Port	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Group ID
					Config	Actual	Config	Actual	
Port.01	1000TX	Up	Enable	Auto	1G Full	1G Full	Disable	OFF	N/A

Port control interface

View the Single Port Information

You can direct click the port on the Switch panel figure on the top of web page. Then, you will see the single port information.



Port information interface

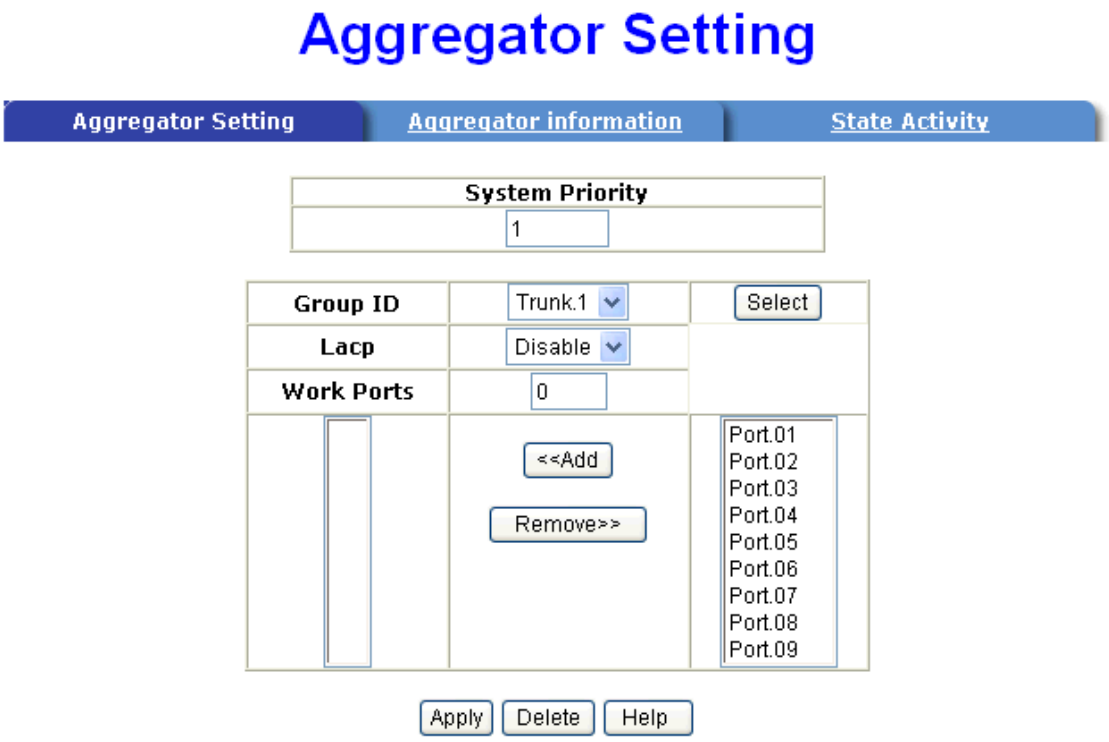
Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to nine consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refers to IEEE 802.3ad.

Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are seven trunk groups to provide configure. Choose the "**Group ID**" and click Select.
3. **LACP:** If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
4. **Work ports:** allow max four ports can be aggregated at the same time. If LACP static trunk group, the exceed ports are standby and able to aggregate if work ports fail. If it is local static trunk group, the number must be as same as the group member ports.
5. Select the ports to join the trunk group. Allow max four ports can be aggregated at the same time. Click Add button to add the port. To remove unwanted ports, select the port and click Remove button.

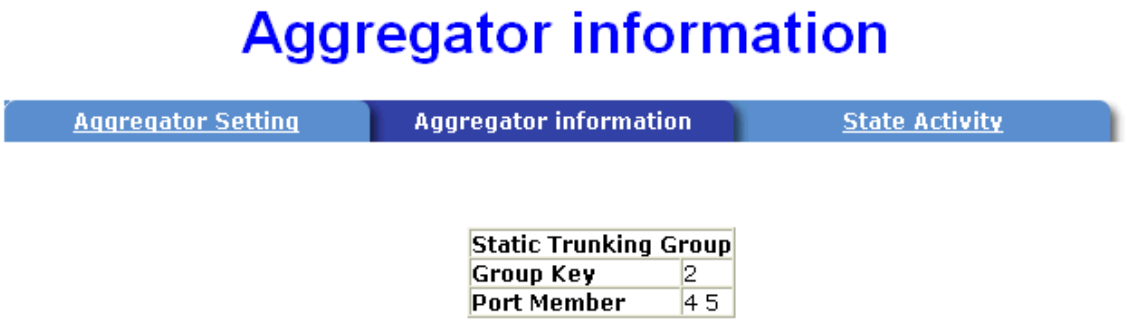
6. If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.
7. Click Apply.
8. Use Delete button to delete Trunk Group. Select the Group ID and click Delete button.



Port Trunk—Aggregator Setting interface

Aggregator Information

When you had setup the LACP aggregator, you will see relation information in here.



Port Trunk – Aggregator Information interface

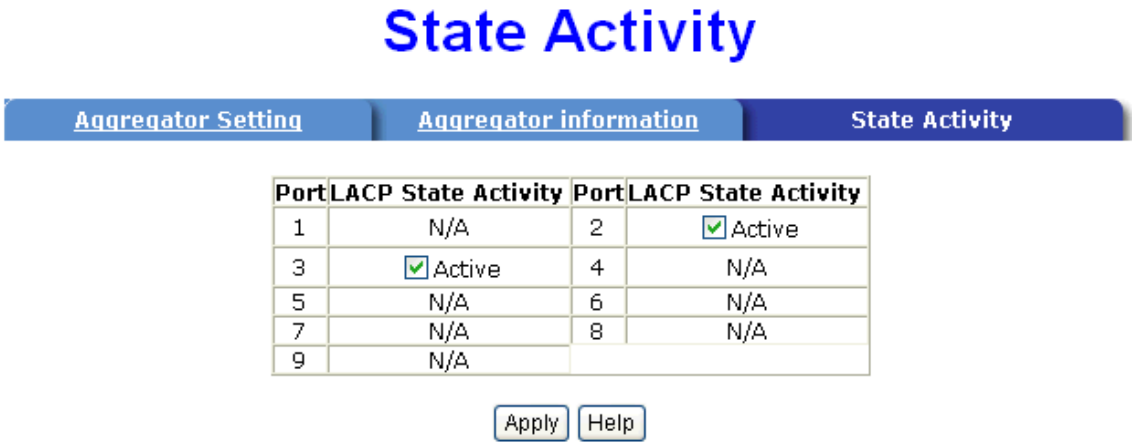
State Activity

When you had setup the LACP aggregator, you can configure port state activity. You can mark or un-mark the port. When you mark the port and click Apply button the port state activity will change to **Active**. Opposite is **Passive**.

4. **Active:** The port automatically sends LACP protocol packets.
5. **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunk.
2. A link has two passive LACP ports will not perform dynamic LACP trunk because both ports are waiting for and LACP protocol packet from the opposite device.
3. If you are active LACP's actor, when you are select trunk port, the active status will be created automatically.



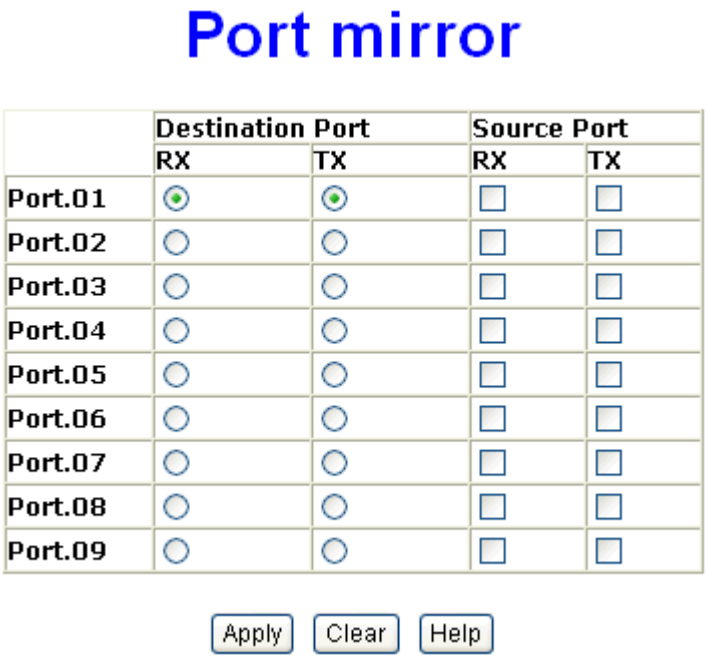
Trunking – State Activity interface

Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic goes in or out monitored ports will be duplicated into mirror port.

1. **Destination Port:** It means mirror port can be used to see all monitor port traffic. You can connect mirror port to LAN analyzer or Netxray. Select the mirroring state – RX, TX or both.
2. **Source Port:** the ports you want to monitor. All monitor port traffic will be copied to mirror port. You can select max 8 monitor ports in the switch. User can choose which port wants to monitor in only one mirror mode. Select the mirrored state – RX, TX or both.
3. Click Apply. If you want to reset the setting, click Clear before apply.

[NOTE] If you want to disable the function, you must select monitor port to none.

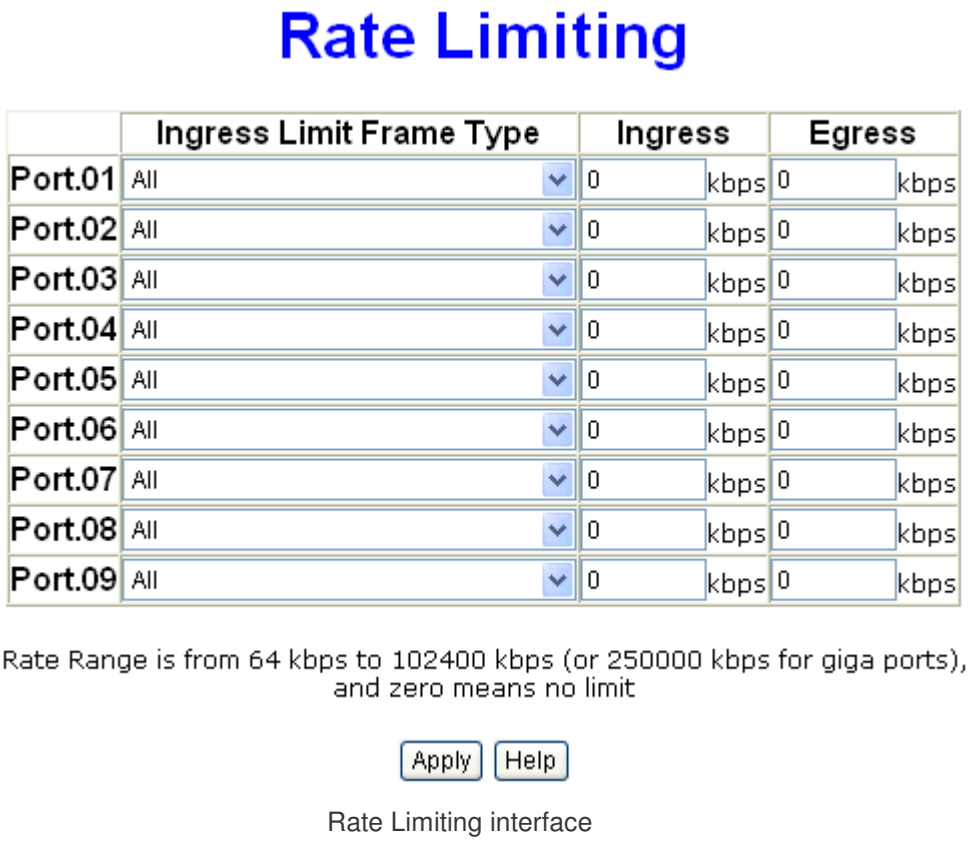


Prot Mirroring interface

Rate Limiting

You can set up every port's bandwidth rate and packet limitation type.

- **Ingress Limit Packet type:** select the packet type that wants to filter. The packet types have all type packet, broadcast/multicast/unknown unicast packet, broadcast/multicast packet, and broadcast packet only. The broadcast/multicast/unknown unicast packet, broadcast/multicast packet, and broadcast packet only are only for ingress packet. The egress rate only supports all type packet.


Rate Limiting
Ingress Limit Frame Type
Ingress
Egress
Port.01 All 0 kbps 0 kbps
Port.02 All 0 kbps 0 kbps
Port.03 All 0 kbps 0 kbps
Port.04 All 0 kbps 0 kbps
Port.05 All 0 kbps 0 kbps
Port.06 All 0 kbps 0 kbps
Port.07 All 0 kbps 0 kbps
Port.08 All 0 kbps 0 kbps
Port.09 All 0 kbps 0 kbps
Rate Range is from 64 kbps to 102400 kbps (or 250000 kbps for giga ports), and zero means no limit
Apply
Help

Rate Limiting interface

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate.
  - **Ingress:** enter the port effective ingress rate. The default value is "0".
  - **Egress:** enter the port effective ingress rate. The default value is "0".
- Click Apply to apply the settings.

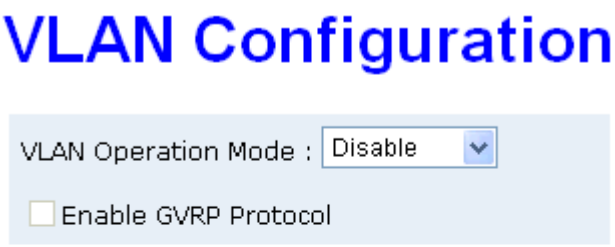
[NOTE] Rate Range is from 64 kbps to 102400 kbps (or 250000 kbps for giga ports) and zero means no limit

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the

same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

The switch supports port-based, 802.1Q (tagged-based) and protocol-base VLAN in web management page. In the default configuration, VLAN support is “disable”.



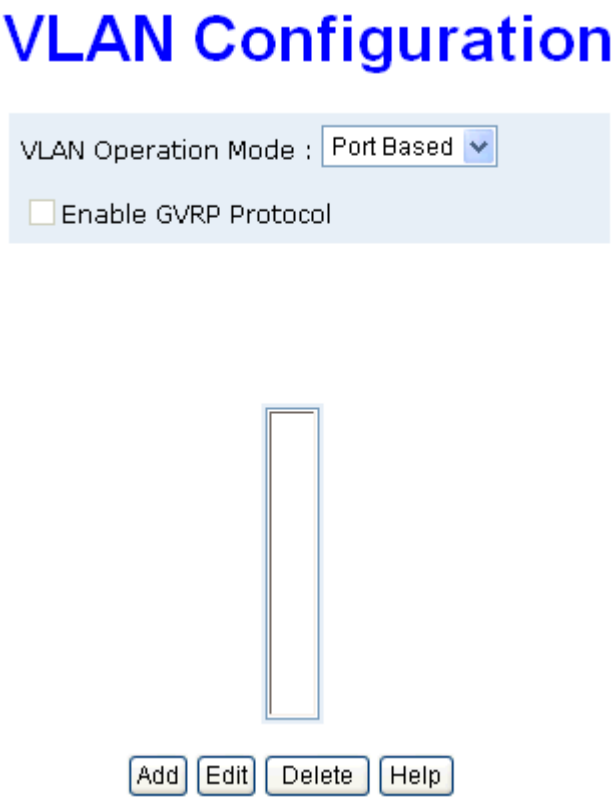
VLAN NOT ENABLE

VLAN Configuration interface

Port-based VLAN

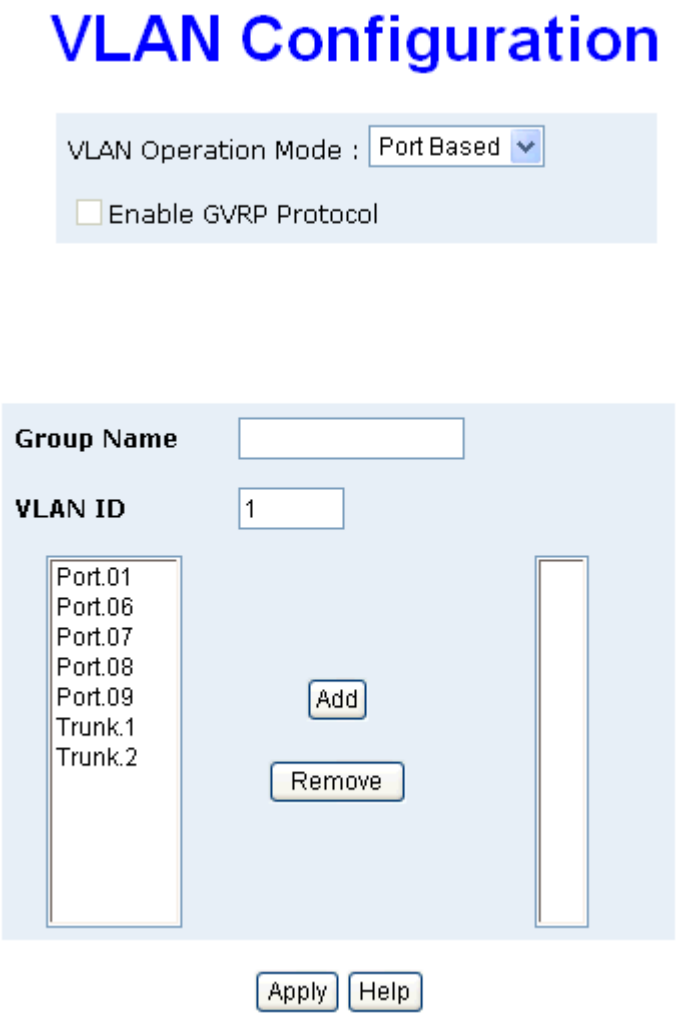
Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLANs, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.



VLAN – PortBase interface

1. Click Add to create a new VLAN group.
2. Enter the Group name, VLAN ID and select the members of VLAN group.
3. Click Apply.



VLAN—PortBase Add interface

4. You will see the VLAN displays.
5. Use Delete button to delete unwanted VLAN.
6. Use Edit button to modify existing VLAN group.

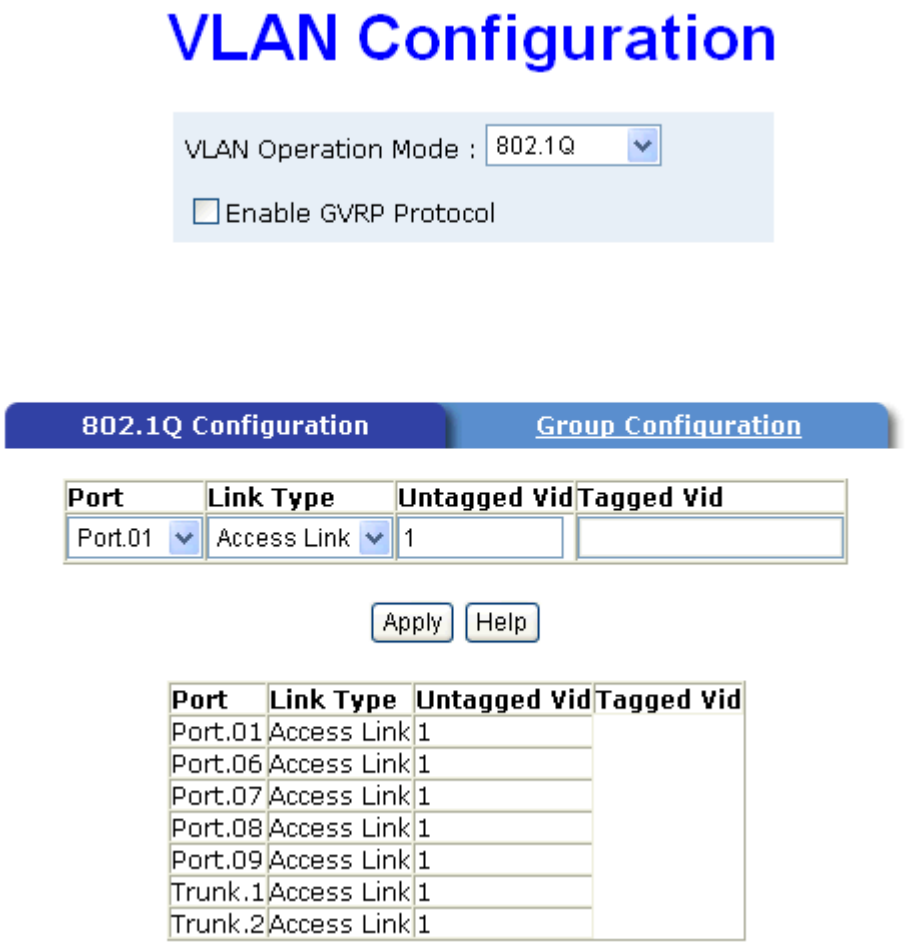
802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID)

that indicates the VLAN numbers.

You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can't be deleting.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



802.1q VLAN interface

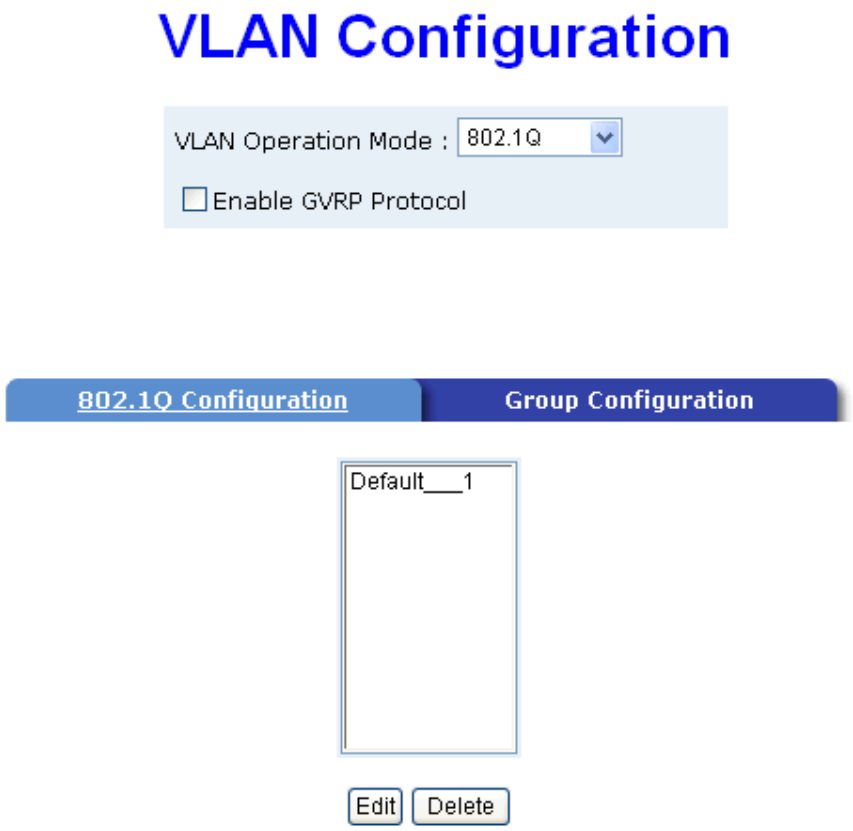
802.1Q Configuration

1. **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
2. Select the port that wants to configure.
3. **Link Type**: there are 3 types of link type.
   - **Access Link:**
   - **Trunk Link:**
   - **Hybrid Link:**
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.
6. Click Apply
7. You can see each port setting in the below table on the screen.

Group Configuration

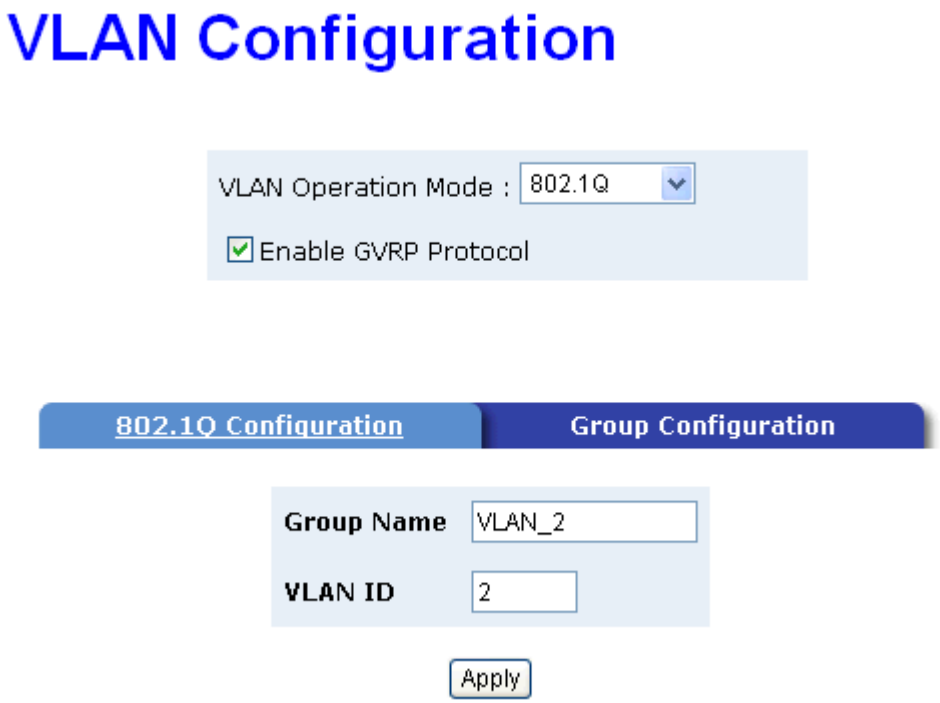
Edit the existing VLAN Group.

1. Select the VLAN group in the table list.
2. Click Apply



Group Configuration interface

3. You can Change the VLAN group name and VLAN ID.
4. Click Apply.



Group Configuration interface

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

RSTP System Configuration

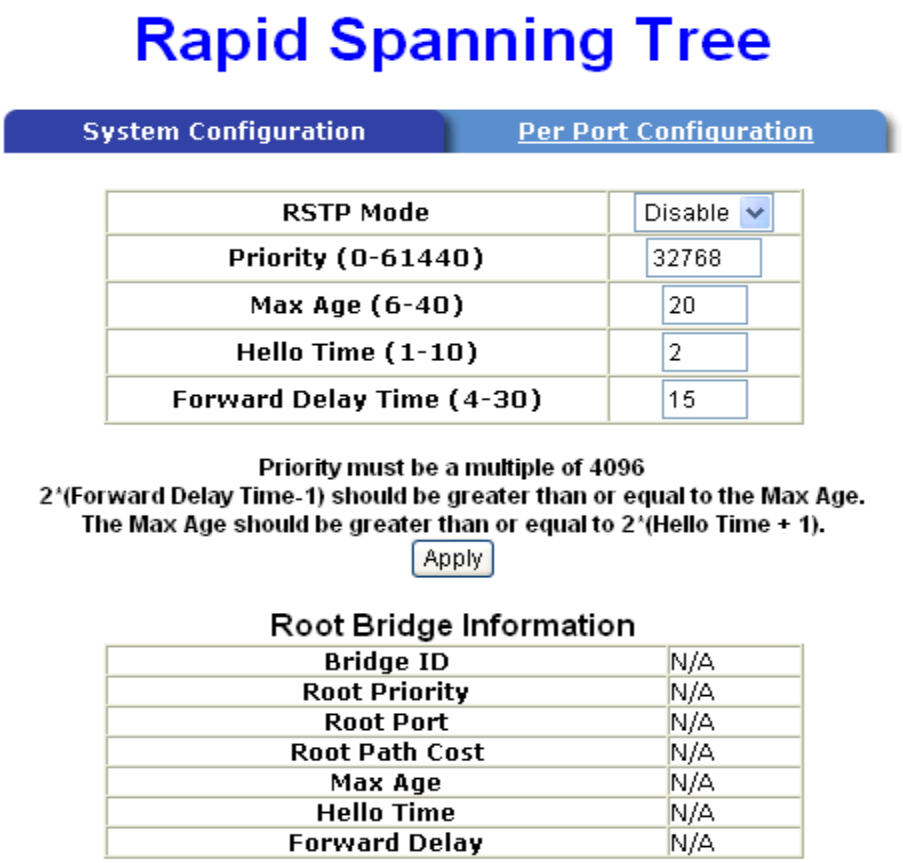
1. You can view spanning tree information about the Root Bridge.
2. You can modify RSTP state. After modification, **save** the configuration.
   - **RSTP mode:** you must enable or disable RSTP function before configure the related parameters.
   - **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If you change

the value, you must reboot the switch assign path priority number. The value must be multiple of 4096 according to the protocol standard rule.

- **Max Age (6-40):** the number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
- **Hello Time (1-10):** the time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
- **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

[NOTE] Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.

2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)



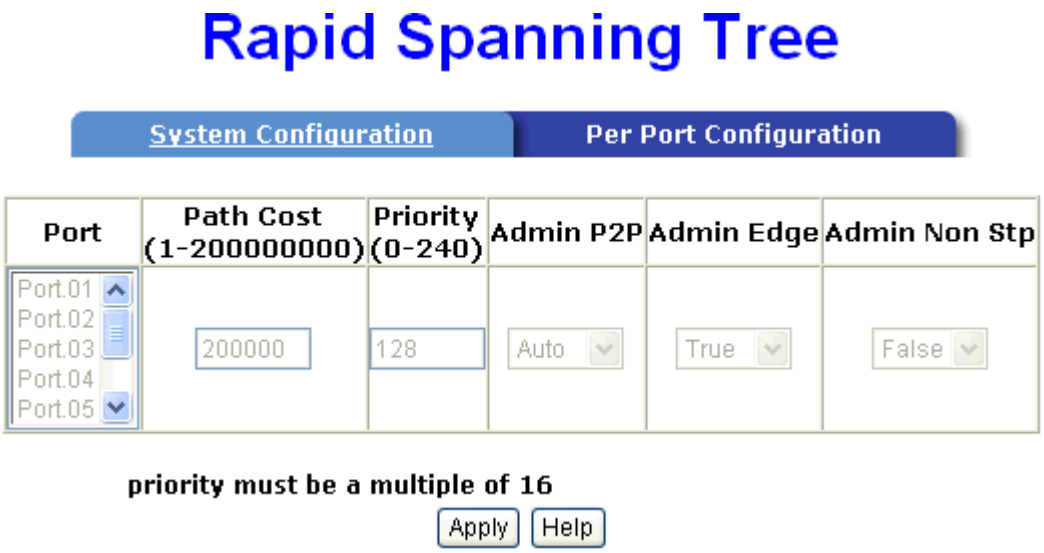
RSTP System Configuration interface

RSTP Per Port Configuration

You can configure path cost and priority of every port.

8. Select the port in Port column.
1. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
2. **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
3. **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.

4. **Edge:** The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
5. **Neighbor:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
6. Click Apply.



RSTP Per Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

- **System Option**

Enter the system name, contact, and location information.

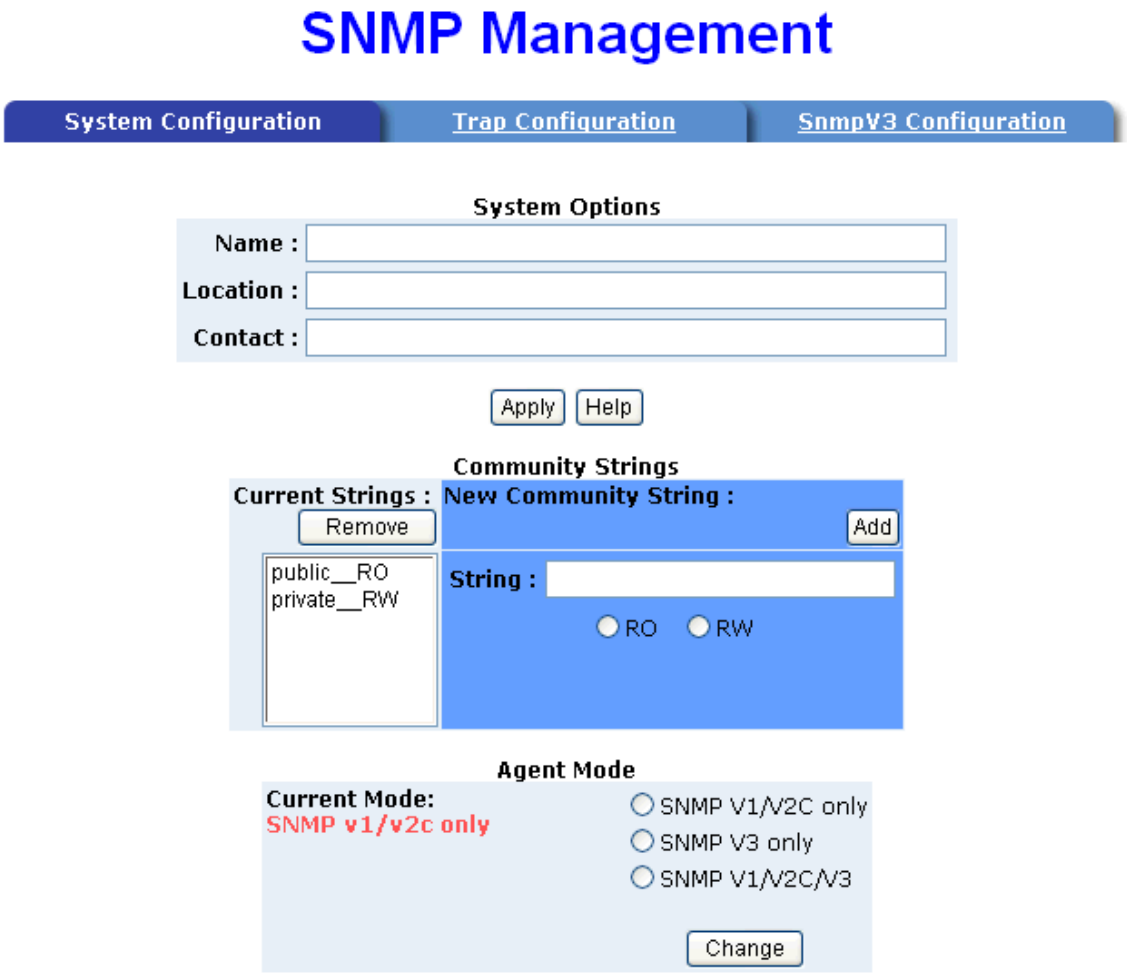
1. **Name:** assign a name for the switch.
2. **Contact:** Type the name of contact person or organization.
3. **Location:** Type the location of the switch.
4. Click Apply.

- **Community Strings**

You can define new community string set and remove unwanted community string.

1. **String:** fill the name of string.
2. **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot remove the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use it. And then click Change to switch to the selected SNMP version mode.



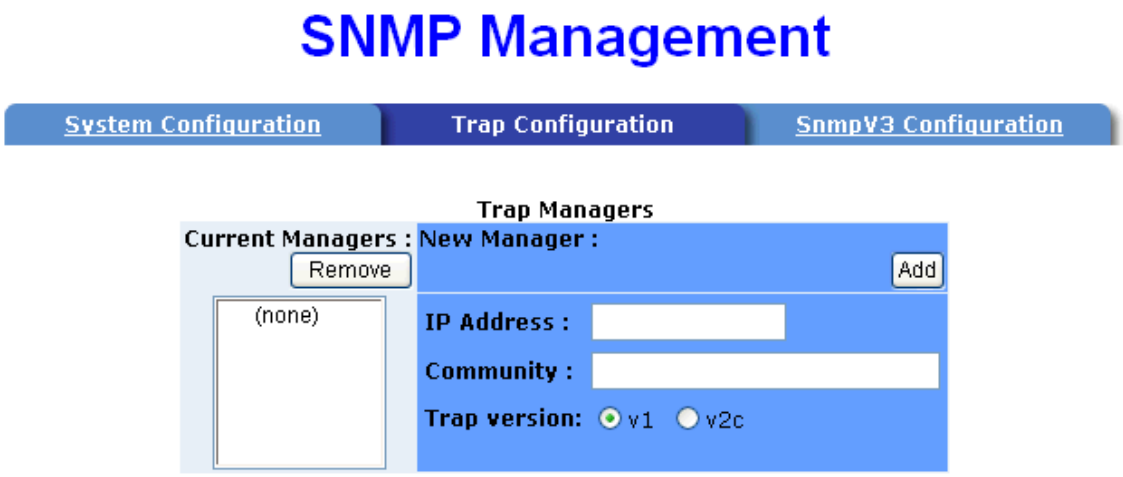
SNMP System Configuration interface

Trap Managers

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

1. **IP Address:** enter the IP address of trap manager.
2. **Community:** enter the community string.

3. **Trap Version:** select the SNMP trap version type – v 1 or v2.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot remove the default community string set.



Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

Context Table

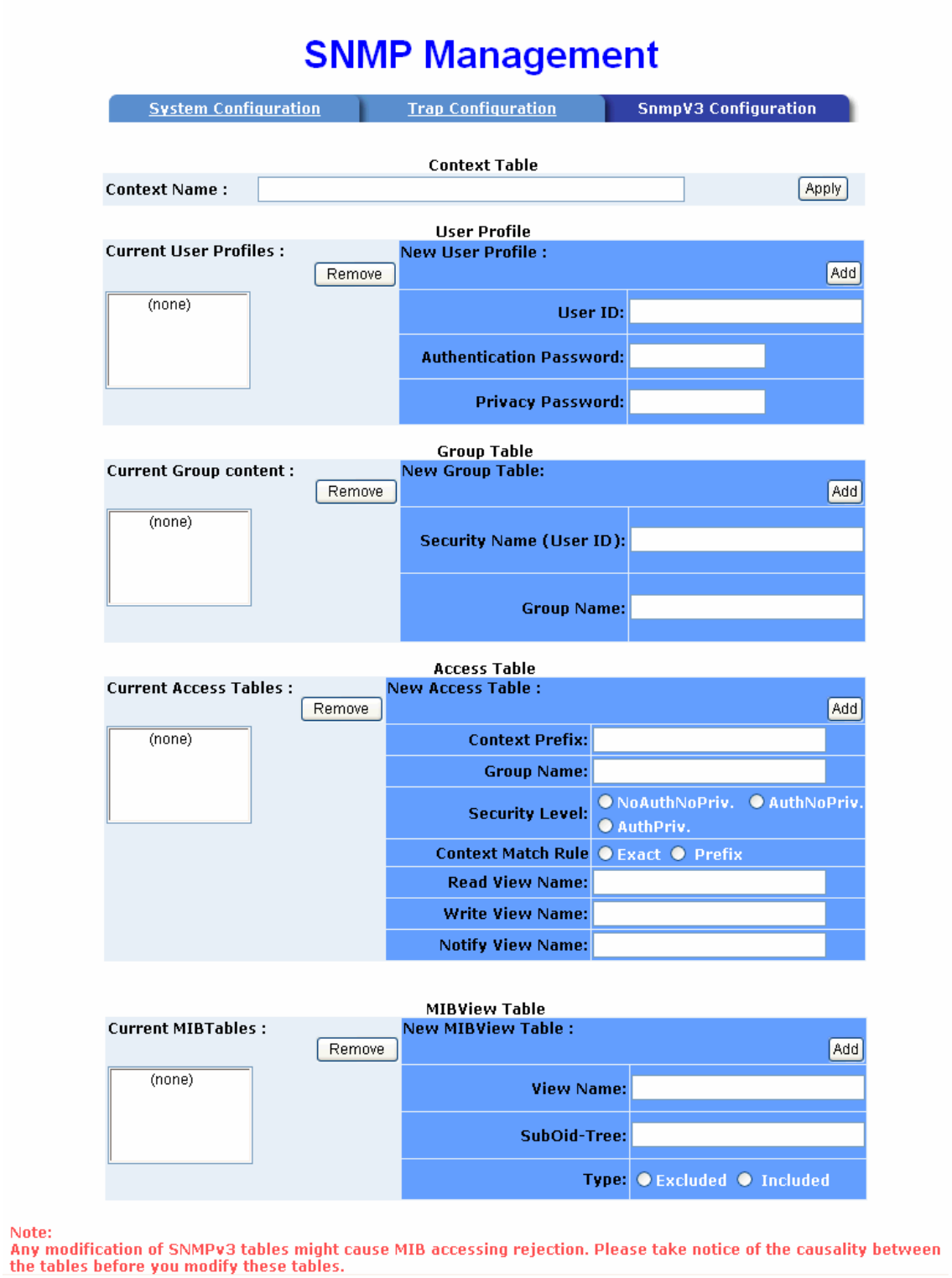
Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name. Click Remove to remove unwanted context name.

User Table

Configure SNMP v3 user table..

- **User ID:** set up the user name.
- **Authentication Password:** set up the authentication password.
- **Privacy Password:** set up the private password.
- Click Add to add context name.

Click Remove to remove unwanted context name.



SNMP V3 configuration interface

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** assign the user name that you have set up in user table.
- **Group Name:** set up the group name.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** set up the context name.
- **Group Name:** set up the group.
- **Security Level:** select the access level.
- **Read View Name:** set up the read view.
- **Write View Name:** set up the write view.
- **Notify View Name:** set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure MIB view table.

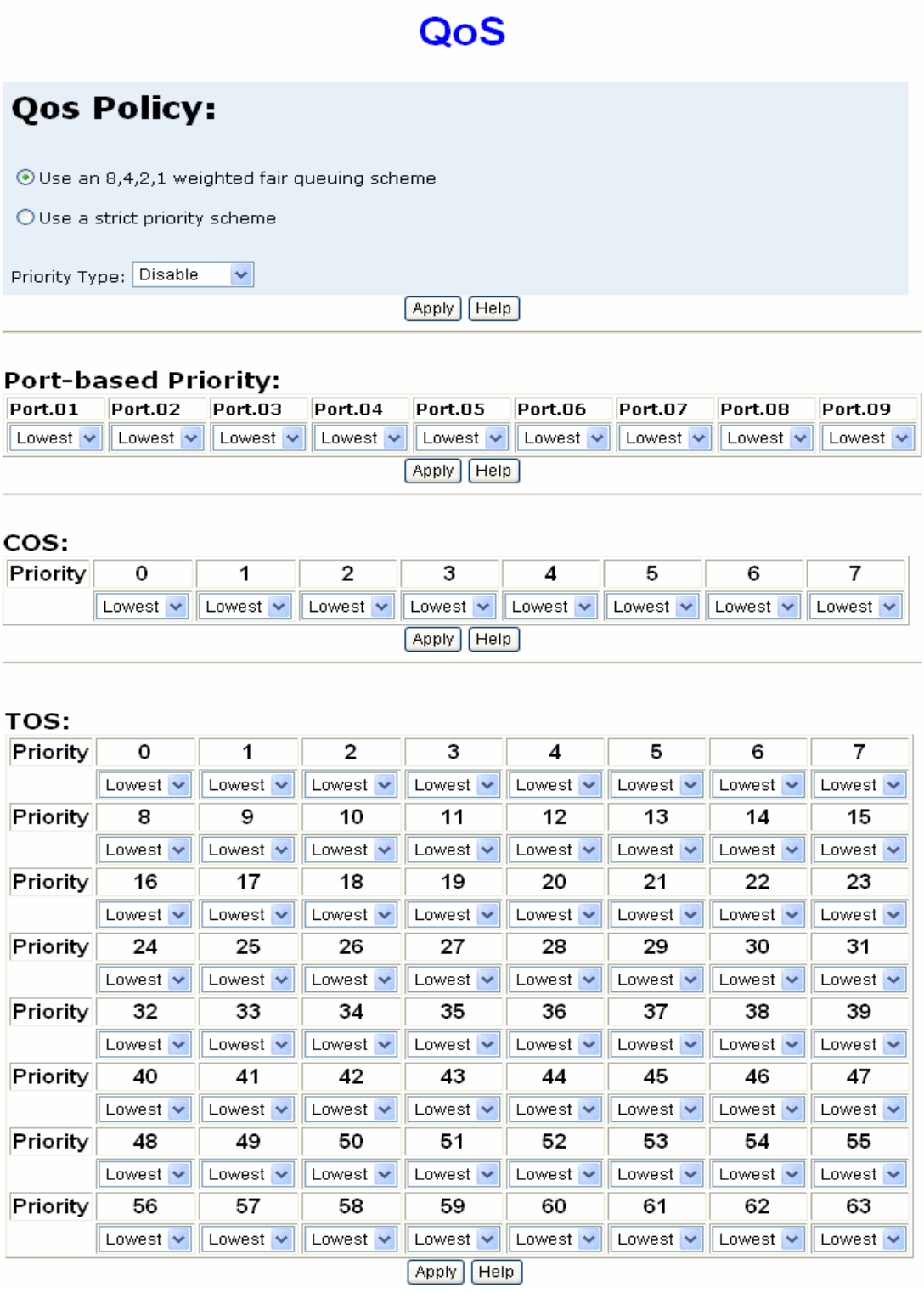
- **ViewName:** set up the name.
- **Sub-Oid Tree:** fill the Sub OID.
- **Type:** select the type – exclude or included.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

QoS Configuration

You can configure Qos policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **Oos Policy:** select the Qos policy rule.
  - **Using the 8,4,2,1 wnine fair queue scheme:** the switch will follow 8:4:2:1 rate to process priority queue from Hi to lowest queue. For example: the system will process 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets at the same time.
  - **Use the strict priority scheme:** Always higher queue will be process first, except higher queue is empty.
- **Priority Type:** every port has 5 priority type selections. Disable means no priority type is selected.
  - **Port-base:** the port priority will follow the **default port priority** that you have assigned – High, middle, low, or lowest.
  - **COS only:** the port priority will only follow the **COS priority** that you have assigned.
  - **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
  - **COS first:** the port priority will follow the COS priority first, and then other priority rule.
  - **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.
- Click Apply.


QoS
Qos Policy:
Use an 8,4,2,1 weighted fair queuing scheme
Use a strict priority scheme
Priority Type: Disable
Apply Help
Port-based Priority:
Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07 Port.08 Port.09
Lowest
Apply Help
COS:
Priority 0 1 2 3 4 5 6 7
Lowest
Apply Help
TOS:
Priority 0 1 2 3 4 5 6 7
Priority 8 9 10 11 12 13 14 15
Priority 16 17 18 19 20 21 22 23
Priority 24 25 26 27 28 29 30 31
Priority 32 33 34 35 36 37 38 39
Priority 40 41 42 43 44 45 46 47
Priority 48 49 50 51 52 53 54 55
Priority 56 57 58 59 60 61 62 63
Lowest
Apply Help

QoS Configuration interface

Port Base Priority

Configure per port priority level.

- **Port 1 ~ G1& 2:** each port has 4 priority levels – High, Middle, Low, and Lowest.
- Click Apply.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has 4 types of priority – high, mid, low, and lowest. The default value is “Lowest” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example: user set the TOS level 25 is high. The port 1 is following the TOS priority policy only. When the port 1 packet received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- Click Apply.

SNTP Configuration

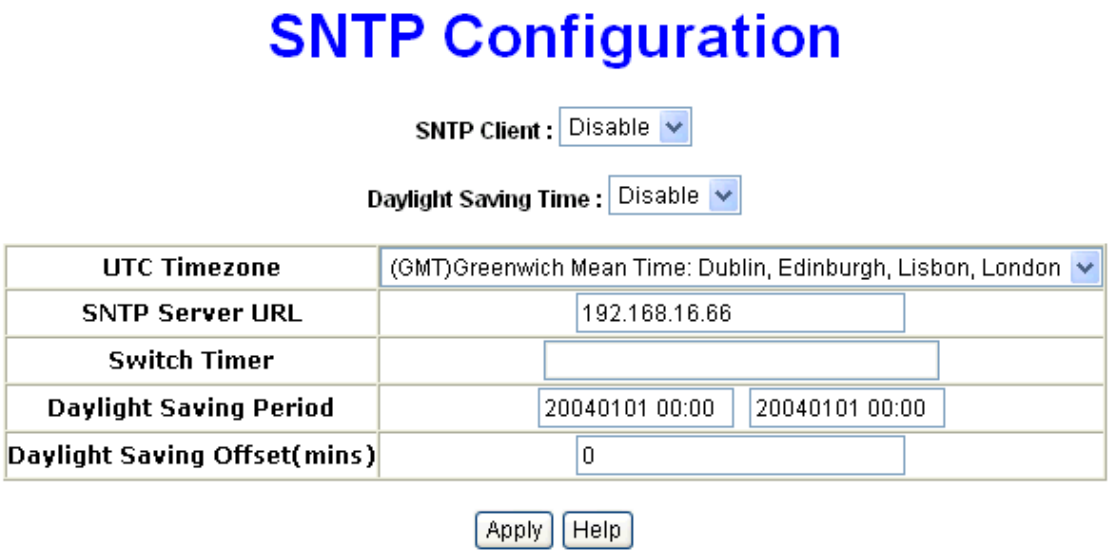
You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period..
3. **UTC Timezone:** set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am

CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. **SNTP Sever URL:** set the SNTP server IP address.
5. **Daylight Saving Period Start:** set up the Daylight Saving beginning time. Daylight Saving benign time will be different in every year.
6. **Daylight Saving Period End:** set up the Daylight Saving ending time. Daylight Saving ending time will different in every year.
7. **Daylight Saving Offset (mins):** set up the offset time.
8. **Switch Timer:** display the switch current time.
9. Click Apply.



SNTP Configuration interface

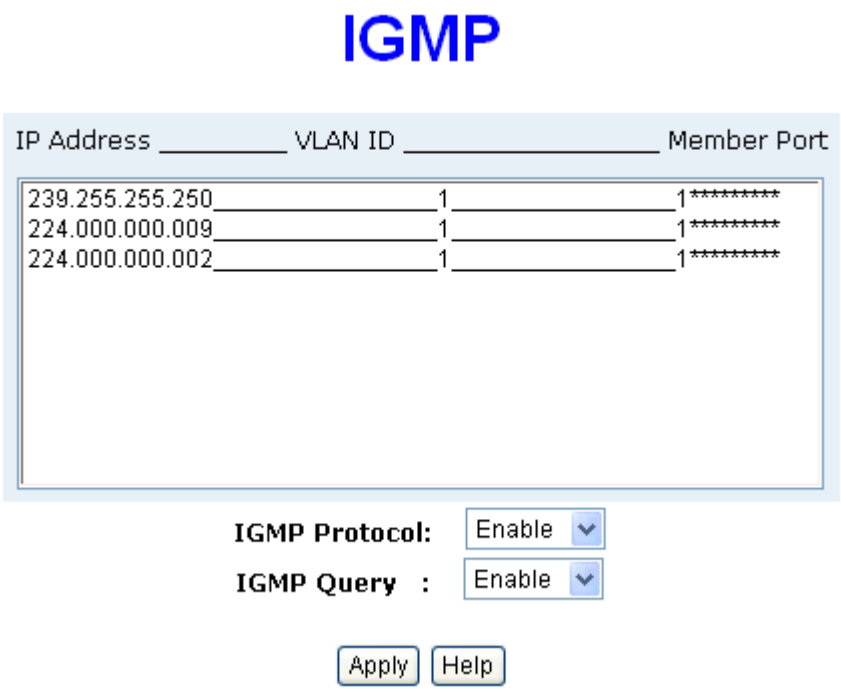
IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then display the IGMP snooping information. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be display in IGMP status section.
- Click Apply.



IGMP Configuration interface

Super ring

Super ring provide a faster redundant recovery than Spanning Tree topology. The action is similar with STP or RSTP, but the algorithms not the same.

In the Super ring topology, every switch should enable super ring function and assign two member ports in the ring. Only one switch in the super ring group would be set as a backup switch that one of two member ports would be blocking, called backup port, and another port is called working port. Other switches are called working switches and their two member ports are called working ports. When the network connection failure, the backup port will automatically become a working port to recovery the failure.

The switch can be set as the ring master or slave. The ring master has the rights to negotiate and place command to other switches in the super ring group. If there are 2 or more switches are in master mode, then software will select the switch with lowest MAC address number as the ring master.

The system also supports the coupling ring that can connect 2 or more super ring group for the redundant backup function.

- **Enable Super ring:** to enable the super ring function.
- **Enable Ring Master:** Enable means the switch is ring master. Disable means the switch is slave.
- **1st & 2nd Ring Port:** select two ports as the member ports. One port will be working port and one port will be the backup port. The system will automatically decide which port is working port and which port is backup port.
- **Enable Coupling Ring:** to enable the coupling ring function.
- **Coupling port:** select the member port.
- **Control port:** select the switch as the master switch in the coupling ring.
- Click Apply.

Super ring Interface

[NOTE] When you enable the super ring function, you must disable the RSTP. The super ring function and RSTP function cannot exist at the same time.

Security Configuration

In this section, you can configure 802.1x, IP, and port security.

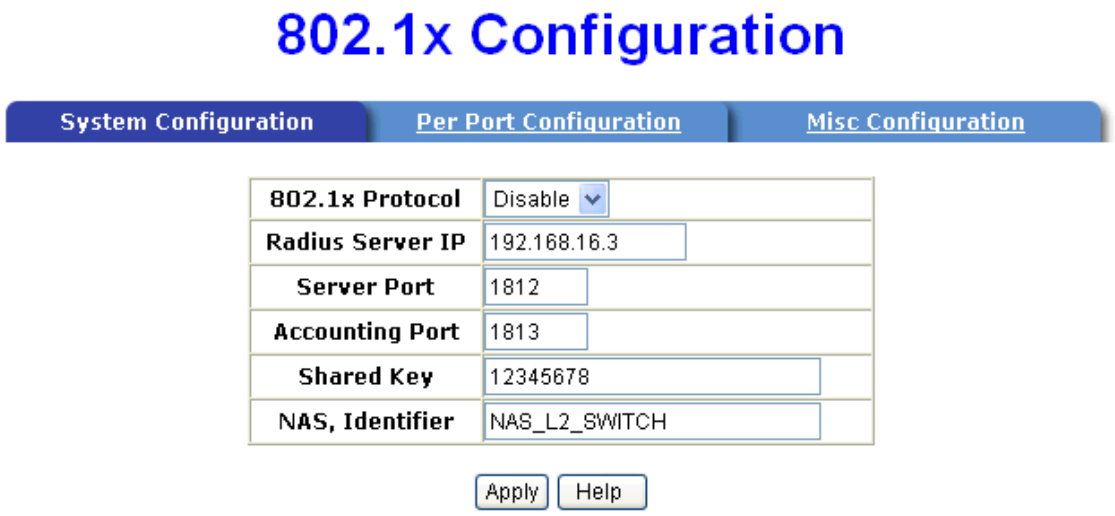
802.1X Configuration

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. **IEEE 802.1x Protocol:** .enable or disable 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
6. **NAS, Identifier:** set the identifier for the radius client.
7. Click Apply.

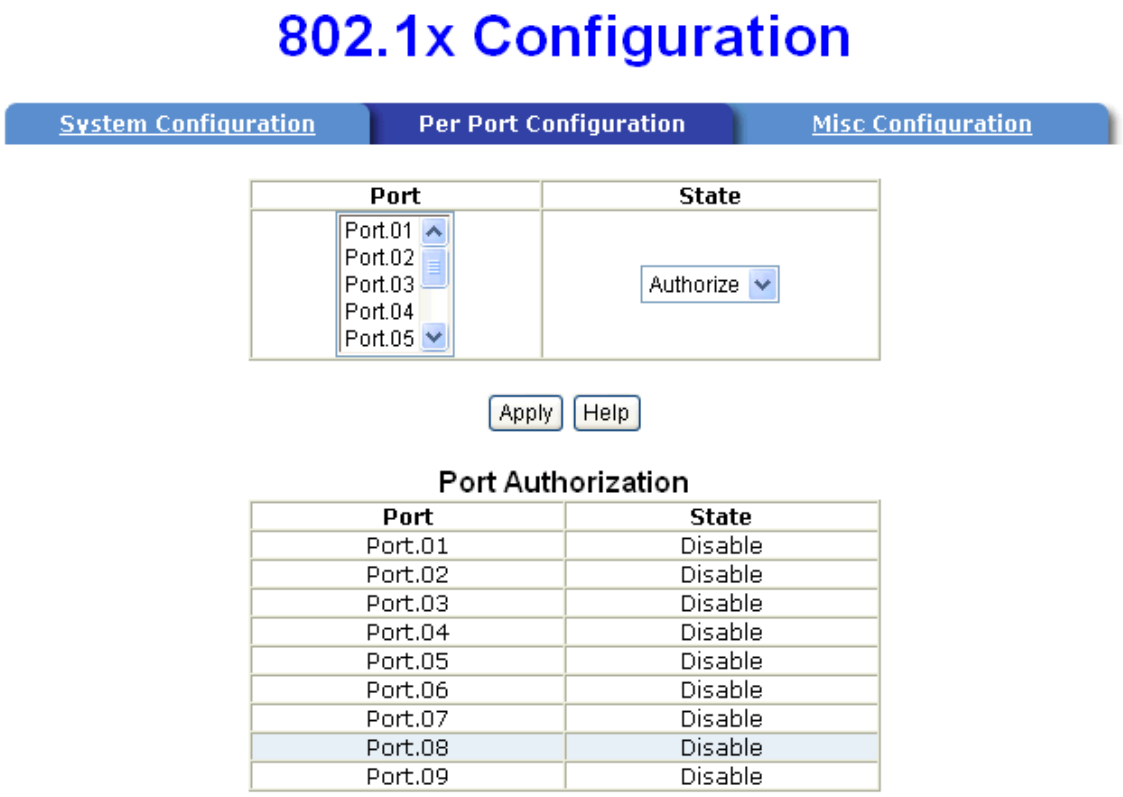


802.1x System Configuration interface

802.1x Per Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use "**Space**" key change the state value.

- **Reject:** the specified port is required to be held in the unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state
- Click Apply.

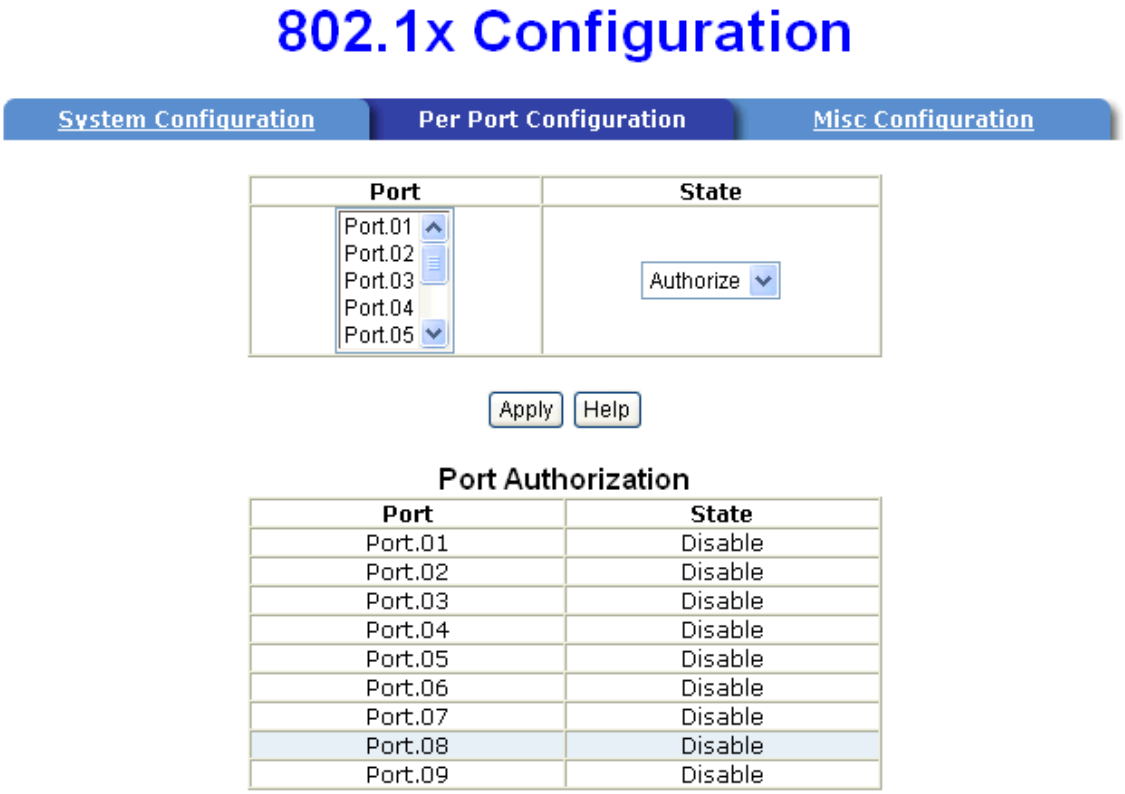


802.1x Per Port Setting interface

Misc Configuration

1. **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.
2. **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
5. **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which clients connected must be re-authenticated.

7. Click Apply.



802.1x Misc Configuration interface

Port Security

Use the MAC address to ensure the port security.

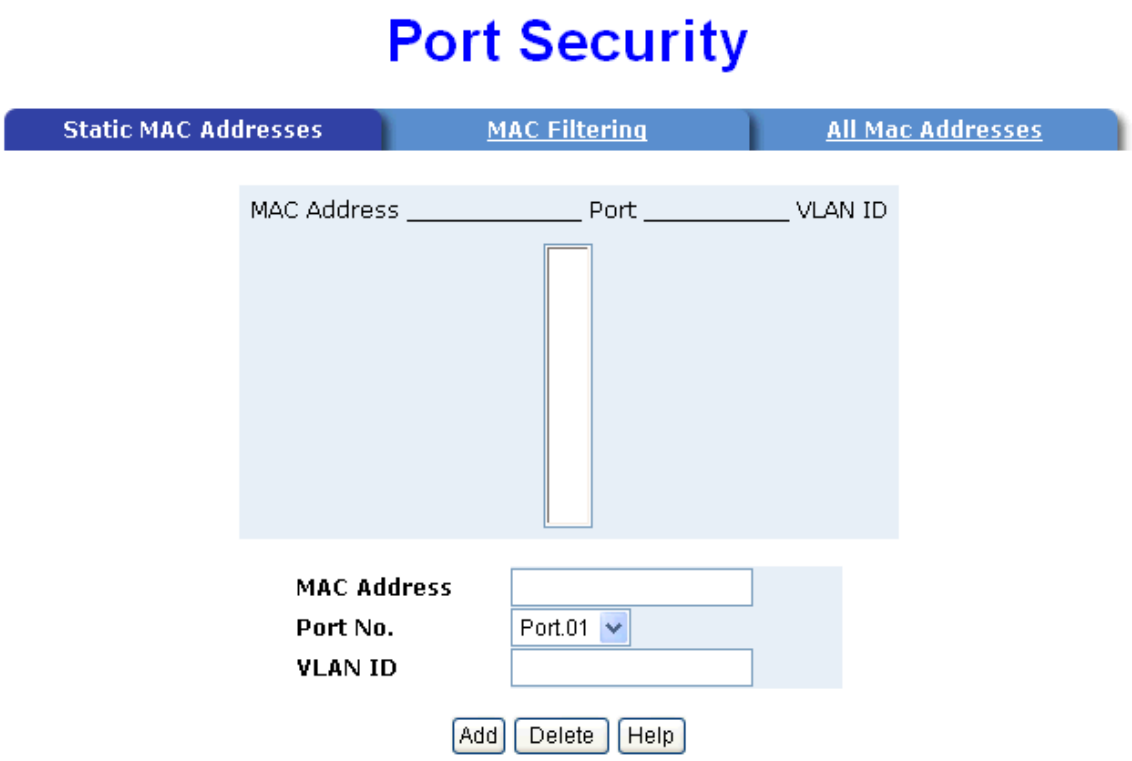
Static MAC Address

You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

- **Add the Static MAC Address**

You can add static MAC address in switch MAC table.

1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
2. **Port No.:** press "**Space**" key to select the port number.
3. **VLAN ID:** enter the Mac address' s VLAD ID, if the Mac address belongs to any VLAN group.
4. Click Add.
5. If you want to delete the MAC address from filtering table, select the MAC address and click Delete.



Static MAC Address interface

Filtering MAC Address

By filtering MAC address, the switch can easily filter pre-configure MAC address and reduce the un-safety. You can add and delete filtering MAC address.

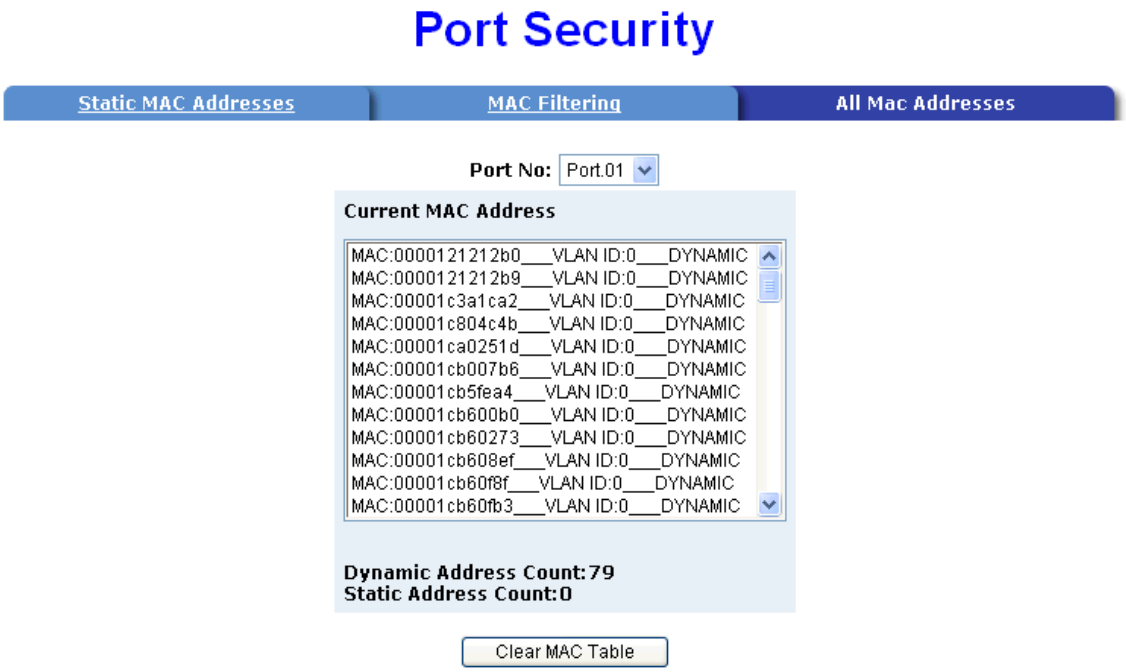
Filtering MAC Address interface

1. **MAC Address:** Enter the MAC address that you want to filter.
2. **VLAN ID:** enter the Mac address's VLAD ID, if the Mac address belongs to any VLAN group.
3. Click Add.
4. If you want to delete the MAC address from filtering table, select the MAC address and click Delete.

All MAC Address

You can view the port that connected device's MAC address and related devices' MAC address.

1. Select the port.
2. The selected port of static MAC address information will display.
3. Click Clear MAC Table to clear the current port static MAC address information on screen.



All MAC Address interface

Factory Default

Reset switch to default configuration. Click Default to reset the all configuration to the default value.

Factory Default interface

Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration will be saved. Click Save Flash to save the all configuration to the flash memory.

Save Configuration interface

System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.

System Reboot interface

Troubleshooting

This section is intended to help you solve the most common problems on the 8 10/100TX plus 1 Gigabit copper & SFP Managed Switch.

Incorrect connections

The switch port can auto detect straight or crossover cable when you link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2-pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ-45 connector is not correct pin on right position then the link will fail. For fiber connection, please notice that fiber cable mode and fiber module should be match.

■ Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. IF that does not correct the problem, try a different cable.

■ Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5-cable tester is a recommended tool for every 100Base-T network installation.

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length does not exceed 100 meters.

■ Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

Diagnosing LED Indicators

The Switch can be easily monitored through panel indicators to assist in identifying problems, which describes common problems you may encounter and where you can find possible solutions.

IF the power indicator does turn on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the Switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. IF you still cannot resolve the problem, contact your local dealer for assistance.

Technical Specifications

This section provides the specifications of switch and the following table lists these specifications.

Standards	IEEE802.3 10BASE-T IEEE802.3u 100BASE-TX IEEE802.3z Gigabit fiber IEEE802.3ab 1000Base-T IEEE802.3x Flow control and Back pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning tree protocol IEEE802.1w Rapid spanning tree IEEE802.1p Class of service IEEE802.1Q VLAN Tagging IEEE 802.1x user authentication
Protocol	CSMA/CD
LED Indicators	System Power (Green) 1000Base-T Port: Speed (100Mbps Green / 1000Mbps Yellow), Link/Activity (Green), SFP: Link/Activity (Green)
Connector	1000Base-T: 9 x RJ-45 Gigabit fiber: 2 x SFP socket. The SFP shared with RJ-45 port 8 and 9.
Switch architecture	Store and forward switch architecture. 18Gbps system backplane. System throughput up to 26.7Mpps.
Packet buffer	1Mbits for packet buffer
RS-232 connector	One RS-232 DB-9 Female connector for switch management
Dimensions	217mm(W) x 140mm(D) x 43mm(H)
MAC Address	8K MAC address table with Auto learning function
Storage Temp.	-10℃~70℃, 95% RH

Operational Temp.	0℃~60℃, 5%~95%RH
Operational Humidity	10% to 90% (Non-condensing)
Power Supply	90~240VAC, 50/60Hz
Power Consumption	10 Watts (Maximum)
Ventilation	Internal Fan
EMI	Compliance with FCC Class A, CE
Safety	Compliance with UL, cUL, CE/EN60950

MILAN BY TRANSITION NETWORKS®

Transition Networks, Inc.
10900 Red Circle Drive
Minnetonka, MN 55343 USA
tel 952.941.7600
or 800.526.9267
fax 952.941.2322
info@transition.com
http://www.transition.com